UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Divisibilidade, Congruência e Aritmética Modular em Problemas Olímpicos

Joselito Elias de Araújo

Trabalho de Conclusão de Curso

Orientador: Prof. Dr. Alciônio Saldanha de Oliveira

Campina Grande - PB
Maio/2018

A663d Araújo, Joselito Elias de.
Divisibilidade, congruência e aritmética modular em problemas olímpicos / Joselito Elias de Araújo. ï Campina Grande, 2018.
108 f. : il. color.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) ï Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2018.
"Orientação: Prof. Dr. Alciônio Saldanha de Oliveira".
Referências.

1. Olimpíadas. 2. Matemática. 3. Teoria dos Números. I. Oliveira, Alciônio Saldanha de. II. Título.

CDU 51(043)

FICHA CATALOGRÁFICA ELABORADA PELO BIBLIOTECÁRIO GUSTAVO DINIZ DO NASCIMENTO CRB - 15/515

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Divisibilidade, Congruência e Aritmética Modular em Problemas Olímpicos

por

Joselito Elias de Araújo

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

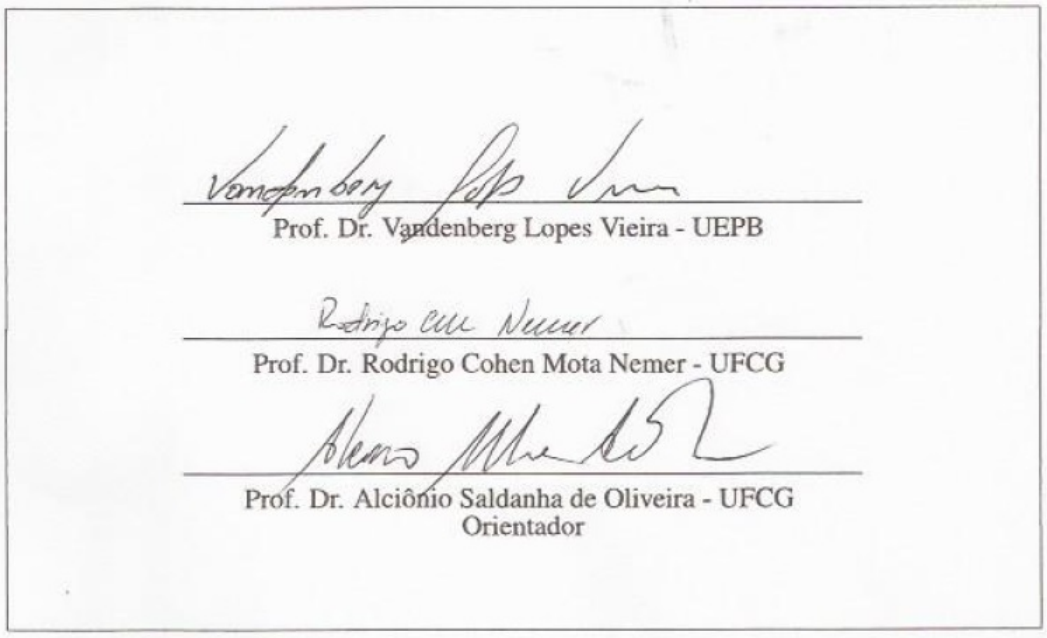
Divisibilidade, Congruência e Aritmética Modular em Problemas Olímpicos

por

Joselito Elias de Araújo

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Aprovado por:



Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Mestrado Profissional em Matemática em Rede Nacional

Abril/2018

Dedicatória

Dedico este trabalho a minha família.

Agradecimentos

Agradeço, primeiramente a Deus, pela vida e a força quem tem me dado todos os dias e as pessoas do meu convívio que acreditaram e contribuíram, mesmo que indiretamente, para a conclusão deste curso.

Aos meus pais José Araújo Filho e Maria Elias de Araújo, pelo amor e pela paciência que tem me doado todo esse tempo. Por terem feito o possível e o impossível para me oferecer a oportunidade de estudar, acreditando e respeitando minhas decisões e nunca deixando que as dificuldades acabassem com os meus sonhos.

A minha esposa Luzineide do Nascimento Silva e ao meu filho Arthur Nascimento Araújo, por terem sentido comigo, todas as angústias e felicidades, acompanhado cada passo de perto. Pelo amor, carinho e apoio depositado, além da companhia por todos esses anos.

Agradeço a meu orientador, Alciônio Saldanha de Oliveira, pela paciência, dedicação, compromisso e ensinamentos que possibilitaram a realização deste trabalho.

A esta universidade e todo seu corpo docente, além da direção e a administração, que realizam seu trabalho com tanto amor e dedicação, trabalhando incansavelmente para que nós, alunos, possamos contar com um ensino de extrema qualidade. Em especial ao coordenador Luiz Antônio da Silva Medeiros.

Agradeço aos meus amigos da turma PROFMAT-UFCG 2016, por confiarem em mim e estarem ao meu lado em todos os momentos, contribuindo com a minha aprendizagem e com palavras de incentivo.

Por fim, agradeço à Sociedade Brasileira da Matemática - SBM pelo oferecimento deste Curso em Rede Nacional.

Resumo

A Matemática é uma ciência viva e em constante construção, não apenas no cotidiano dos indivíduos, mas também nas universidades. Neste sentido, com objetivo de difundir o conhecimento matemático tanto no Ensino Básico quanto no Ensino Superior, foram criadas as Olimpíadas de Matemática, um projeto em âmbitos internacional, nacional, regional e local, que tem a finalidade de estimular e promover o estudo da Matemática, desta forma contribuindo para uma educação básica de qualidade. No presente trabalho abordamos um pouco sobre a origem das Olimpíadas de Matemática, discorremos sobre o surgimento e os objetivos das principais olimpíadas, alguma internacionais: Olimpíada Internacional de Matemática (IMO); Ibero-Americana de Matemática; Cone Sul e a Olimpíada de Maio e nacionais: Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) e a Olimpíada Brasileira de Matemática (OBM) e, regionalmente, falamos sobre a Olimpíada Campinense de Matemática (OCM), olimpíada promovida e realizada pela Universidade Federal de Campina Grande (UFCG). Em consonância com os problemas abordados por estas competições, abordamos alguns conceitos relacionados à Teoria do Números, tais como divisibilidade, congruências e aritmética modular. Este trabalho visa justificar a necessidade da construção de um material de apoio que contemple professores e alunos de escolas públicas e privadas que tenham interesse em se preparar para as Olimpíadas de Matemática. A intenção não é usar este material como um curso de olimpíadas, pois ele está muito longe de ser completo, mas pode ser utilizado para revisar alguns tópicos importantes relacionados à Teoria do Números.

Palavras Chaves: Olimpíadas. Matemática. Teoria dos Números.

Abstract

Mathematics is a living and constantly growing science, not only in the everyday life of individuals, but also in universities. In this sense, in order to disseminate mathematical knowledge in both Basic and Higher Education, the Mathematical Olympiads were created, a project at the international, national, regional and local levels, with the purpose of stimulating and promoting the study of Mathematics , thus contributing to a quality basic education. In the present work we approach a little about the origin of the Mathematical Olympiads, we discuss about the emergence and the objectives of the main olympiads, some international: International Mathematical Olympiad (IMO); Ibero-American Mathematics; South Cone and the Olympiad of May and national: Brazilian Olympiad of Mathematics of the Public Schools (OBMEP) and the Brazilian Mathematical Olympiad (OBM) and, regionally, we talked about the Olympiad Campinense de Matemática (OCM), Olympiad promoted and held by the University Federal University of Campina Grande (UFCG). In line with the problems addressed by these competitions, we have dealt with concepts related to Number Theory such as divisibility, congruences and modular arithmetic. This paper aims to justify the need to construct a support material that includes teachers and students from public and private schools interested in preparing for the Mathematical Olympiads. The intention is not to use this material as an olympics course, as it is far from complete, but can be used to review some important topics related to Number Theory.

Keywords: Olympiads. Mathematics. Theory of Numbers.

Sumário

Capítulo 1

Introdução

Um importante projeto que vem sendo desenvolvido no Brasil é as Olimpíadas Científicas [1], com objetivo de incentivar e encontrar talentos nas diversas áreas do conhecimento. Tais Olimpíadas são muito diversas: existem Olimpíadas de Matemática, Química, Física, História, Linguística, Biologia, Astronomia, Oceanografia, Informática, dentre outras. Algumas consistem de provas teóricas, outras consistem em fazer programas, experimentos, e até mesmo debates.

Neste contexto, discorremos sobre algumas das principais Olimpíadas de Matemática, nacionais e internacionais. No cenário nacional, escolhemos a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) e a Olimpíada Brasileira de Matemática (OBM). Também falamos um pouco sobre a Olimpíada Campinense de Matemática (OCM), Olimpíada regional promovida e realizada pela Universidade Federal de Campina Grande (UFCG). No âmbito internacional, falamos um pouco sobre a Olimpíada Internacional de Matemática (IMO), Ibero-Americana de Matemática, Cone Sul e a Olimpíada de Maio.

Para Jacob Palis, pesquisador do Instituto de Matemática Pura e Aplicada (IMPA) na introdução do livro de Moreira [9]:

> As Olimpíadas de Matemática são hoje reconhecidamente um poderoso instrumento não só para a descoberta de talentos, mas também para difusão desta área fundamental do conhecimento, a que são expostas nossas crianças desde bem cedo. De fato, quando organizadas em várias etapas ou fases para o mesmo grupo de crianças ou jovens, pode-se ir desde testes amigáveis e atraentes até a etapa mais seletiva da descoberta de talentos, muitos deles tornando-se mais tarde excelentes cientistas ou profissionais em geral, (MOREIRA 2003, p.175).

No presente trabalho, temos como objetivo trabalhar alguns tópicos da Teoria dos Números, os quais se enquadram no ramo denominado posteriormente de *Teoria Elementar*, ou seja, iremos estudar tópicos relacionados a *Divisibilidade* e *Congruências*, enfatizando a importância desses conteúdos que estão diretamente envolvidos em Olimpíadas de Matemática.

[1] Competições para estudantes do ensino fundamental e médio, podendo também incluir alunos de graduação, em qualquer período.

A aritmética, como usualmente é chamada a parte elementar da Teoria dos Números, teve como principal marco inicial a obra *Os Elementos*, de Euclides (aprox. 300 a.C.), encontrando o seu auge nos trabalhos de Pierre de Fermat (1601 - 1665) e Leonhard Euler (1707 - 1783), o que a levou a tornar-se um dos principais pilares da Matemática. A partir do início do século XIX, graças à obra de Carl Friedrich Gauss (1777 - 1855), a Aritmética transforma-se em Teoria dos Números e começa a ter um desenvolvimento extraordinário.

A Teoria dos Números dedica-se ao estudo dos números inteiros e suas generalizações. Em geral, tal estudo está relacionado com soluções de problemas diofantinos, ou seja, problemas que requerem solução de equação ou de sistemas de equações com valores inteiros para as suas incógnitas. Entre os seus vários ramos, três têm destaque especial: a *Teoria Algébrica*, a *Teoria Analítica* e a *Teoria Elementar*. Em outras palavras, é possível observar o estudo dos números inteiros sob ao menos três pontos de vista diferentes.

Na *Teoria Algébrica*, estuda-se os números algébricos (números complexos que são raízes de polinômios não nulos com coeficientes racionais) e considera resultados da Álgebra Abstrata a fim de resolver as questões inerentes. A *Teoria Analítica* emprega resultados da Análise Matemática, tanto real como complexa, quando do estudo mais aprofundado sobre os números primos. Por último, a *Teoria Elementar*, cujos tópicos estudados se constituem num primeiro contato dos estudantes com as propriedades dos números inteiros, tem por objetivo estudar os conceitos e resultados básicos sobre divisibilidade, Primalidade, congruência entre inteiros, dentre outros.

Estruturalmente, nosso trabalho está organizado em 5 (cinco) capítulos, além da introdução (capítulo 1) e das considerações finais (capítulo 7). São eles:

- Capítulo 2: realizamos um breve histórico sobre os principais protagonista que transformaram a Aritmética em Teoria dos Números.

- Capítulo 3: apresentamos a origem e os caminhos das Olimpíadas de Matemática e passeamos pela história das principais Olimpíadas de Matemática realizadas nacionalmente e internacionalmente; apresentamos também um guia de estudo que jugamos ser importante para um bom desempenho em Olimpíadas de Matemática.

- Capítulo 4: abordamos conceitos, relacionados à Indução Matemática, Divisibilidade, Máximo Divisor Comum (MDC), Mínimo Múltiplo Comum (MMC) e Números Primos.

- Capítulo 5: exibimos conceitos e definições associados à Congruências e aos Teoremas de Wilson, Fermat e Euler.

- Capítulo 6: mostramos algumas aplicações que relacionem os conteúdos estudados nos capítulos 4 e 5 com as questões abordadas nas provas das Olimpíadas de Matemática nacionais citadas anteriormente, além de problemas extraídos do Banco de

Questões da OBMEP - 2017 e do material elaborado pelo programa Polos Olímpicos de Treinamento Intensivo (POTI).

1.1 Objetivos

1.1.1 Objetivo Geral

Nosso trabalho tem como objetivo principal elaborar um material na área de aritmética, que possa auxiliar professores e estudantes envolvidos em Olimpíadas de Matemática.

1.1.2 Objetivos Específicos

- Apresentar alguns teoremas da aritmética como ferramentas para resolver problemas olímpicos;
- Mostrar a importância da aritmética nas provas de Olimpíadas de Matemática;
- Mostrar como as Olimpíadas de Matemática podem contribuir para visibilidade da Matemática e como ela pode despertar o interesse de mais alunos por essa disciplina;
- Contribuir para o ensino-aprendizagem da aritmética na educação básica;
- Historiar as Olimpíadas de Matemática.

Capítulo 2

Protagonistas na Teoria dos Números - Histórico

2.1 Euclides de Alexandria

Euclides de Alexandria professor, escritor, muitas vezes é referido como o "Pai da Geometria", foi um dos matemáticos mais importantes da Grécia Clássica e de todos os tempos. Sua obra *Os Elementos* é uma das mais influentes na história da matemática, servindo como o principal livro para o ensino de matemática (especialmente geometria) desde a data da sua publicação até o fim do século XIX ou início do século XX. Nessa obra, os princípios do que é hoje chamado de geometria euclidiana foram deduzidos a partir de um pequeno conjunto de axiomas. Euclides também escreveu obras sobre perspectiva, seções cônicas, geometria esférica e teoria dos números.

Euclides nasceu na Síria aproximadamente em 330 a.C. e realizou seus estudos em Atenas. Sobre sua vida pessoal, não tem-se muitos relatos. Sabe-se que ele foi convidado a lecionar Matemática na escola instituída em Alexandria por Ptolomeu I, governante do Egito de 323 a.C. a 283 a.C. Nesta escola, Euclides se destacou entre os demais professores pelo método utilizado em suas aulas de Geometria e Álgebra. Sua maneira indicava que ele tinha um grande potencial para explanar as disciplinas que lecionava.

Depois de convidado para compor o quadro de professores da recém fundada Academia que tornaria Alexandria no centro do saber da época, Euclides tornou-se o mais importante autor de Matemática da Antiguidade greco-romana e, talvez, de todos os tempos, com sua monumental obra *Os Elementos*, no estilo livro de texto, foi sua primeira obra, dividida em treze volumes[1], sendo:

> (i) cinco sobre geometria plana. (ii) três sobre números. (iii) um sobre a teoria das proporções. (iv) um sobre incomensuráveis. (v) três (os últimos) sobre geometria no espaço.

[1] http://clubes.obmep.org.br

Escrita em grego, a obra cobria toda a aritmética, a álgebra e a geometria conhecidas até o momento, reunindo o trabalho de seus predecessores, como Hipócrates e Eudóxio. Sistematizava todo o conhecimento geométrico dos antigos e intercalava os teoremas já conhecidos com a demonstração de muitos outros, que completavam a obra e davam coerência e encadeamento lógico ao sistema por ele criado. Após sua primeira edição, foi copiado inúmeras vezes e, versado para o árabe, tornou-se o mais influente texto científico de todos os tempos e um dos com maior número de publicações ao longo da história. A teoria aí desenvolvida é uma das mais importantes na trajetória da Matemática, o que levou este livro a ser adotado como prioridade nas aulas desta disciplina, particularmente as de geometria, desde o momento em que foi lançado até fins do século XIX ou princípio do século XX. Esta teoria se tornou conhecida como Geometria Euclidiana.

2.2 Pierre de Fermat

Pierre de Fermat foi advogado e oficial do governo em Toulouse pela maior parte de sua vida. Nascido na França, na primeira década do século XVII. A Matemática era o seu passatempo. Seu pai era um rico mercador, e lhe propiciou educação privilegiada.

Seu interesse pela Matemática se iniciou com a leitura de Aritmética de Diofanto, obra que seria responsável pela divulgação de um dos maiores problemas Matemáticos que o mundo conheceu. A sua influência foi limitada por não ter interesse em publicar suas descobertas, conhecidas principalmente por cartas de amigos, e por sua cópia da Aritmética de Diofanto, que chegou a receber uma versão especial (Aritmética de Diofanto contendo observações de Pierre de Fermat), onde foram impressas todas as notas de Fermat. Em suas cartas, ele descrevia ideias, descobertas e até pequenos ensaios. Era um matemático que gostava de trocar e resolver desafios.

É considerado o *Príncipe dos Amadores*, pois nunca teve a Matemática como principal atividade na sua vida, dedicando-se à ela em horas de lazer. Mesmo assim, chegou a ser considerado o maior matemático de seu tempo. Fermat ajudou na criação da Geometria Analítica, em 1629, descrita em um trabalho não publicado (Introdução aos lugares geométricos planos e sólidos). Teve circulação apenas em forma de manuscrito, e mostrava equações gerais da reta, circunferência, e equações mais simples para parábolas, elipses e hipérboles. Partes dessa obra, como o seu método para estabelecer tangentes, foram usados por grandes cientistas, como Isaac Newton.

Também contribuiu com a Teoria da Probabilidade, que desenvolveu junto com Pascal, enquanto trocavam cartas. Ambos determinaram as regras essenciais da probabilidade. Porém, esse não era seu maior interesse apenas resolvia os problemas a respeito de probabilidade que lhe eram propostos por Pascal. Seu maior interesse era na Teoria dos Números, e em jogos com números, que ele criava, e desafiava outros matemáticos a resolverem.

Foi dele, também, o estudo de eixos perpendiculares, base das coordenadas cartesianas,

cujo estudo é atribuído a René Descartes.

2.3 Leonhard Paul Euler

Leonhard Paul Euler nasceu na Basiléia ao norte da Suíça, quase na fronteira com a França, no dia 15 de abril de 1707. Filho de Paul Euler, um pastor protestante Calvinista, e de Margarete Brucker, Euler foi educado inicialmente por seu próprio pai. Começou estudos em Teologia em 1720 na Universidade da Basiléia.

Posteriormente, estudou Matemática, tendo como tutor Johann Bernoulli, o que foi importante para que Euler seguisse a carreira de matemático. Quando tinha 19 anos, apresentou como tese para a cátedra de física uma memória denominada "Dissertação Física sobre o Som". Apesar do fracasso em obter o título, esse panfleto tornou-se um clássico e serviu de guia à pesquisa em acústica no resto do século. Ele contribuiu mais à acústica teórica que qualquer outra pessoa.

Em 1727, mudou-se para São Petersburgo, Rússia. Casou-se em 1734 e teve 13 filhos, dos quais apenas 5 sobreviveram. Consta que Euler declarou uma vez que suas principais criações matemáticas ocorreram quando tinha um bebê e crianças próximas.

Os primeiros problemas de saúde de Euler surgiram em 1735. Em 1738, ele perdeu a visão de seu olho direito. Em 1766, teve catarata e perdeu a vista no olho esquerdo. Sua deficiência não o impediu, entretanto, de ser o matemático mais produtivo de todos. Antes, em 1741, mudou-se para a Alemanha. Retornou a São Petersburgo em 1766, pouco antes de perder sua visão, onde permaneceu até falecer com 76 anos em 7 de setembro de 1783.

2.4 Jonhann Carl Friedrich Gauss

Jonhann Carl Friedrich Gauss foi um matemático, astrônomo e físico alemão. O nome de Gauss está associado a uma grande parte de *Teoria dos Números Clássicos*. Ele resolveu perguntas em aberto, como a reciprocidade quadrática, conjecturou o Teorema de Número Primo e escreveu o seu livro monumental quando tinha 21 anos. Gauss é considerado um gênio e também um grande matemático. Ele também deu grandes contribuições na física, onde previu a existência da geometria não Euclidiana. Chamado de o "Príncipe dos Matemáticos", publicou uma obra fundamental para a moderna Teoria dos Números, *Disquisitones Arithmeticae*, em que desenvolveu a álgebra da relação de congruência. Com essa obra, a Teoria dos Números se transformou em uma nova disciplina dotada de métodos próprios, mais profundos, fonte e modelo para as teorias aritméticas do século XIX. Em 1825, ele introduziu os números inteiros gaussianos (números complexos da forma $a+bi$, onde a e b são números inteiros e $i^2 = -1$), uma extensão da ideia de número primo, pois descobriu que muito da antiga teoria de Euclides sobre fatoração de inteiros poderia ser transportada para esse conjunto com consequências importantes para a Teoria dos Números.

Capítulo 3

Origem e Caminhos das Olimpíadas de Matemática

O que é uma Olimpíada de Matemática? É uma sequência de provas, envolvendo apenas resolução de problemas de Matemática. Os participantes são alunos que estão matriculados em escolas de ensino fundamental e médio, ou em cursos universitários. Usualmente, os problemas exigem muita capacidade de criar e improvisar.

Os alunos que fazem mais pontos ganham medalhas, menções honrosas e, em alguns casos, pequenas quantias de dinheiro como parte da premiação. Claro que o que mais importa é o prazer de se superar e confraternizar com colegas de outras escolas. No caso de olimpíadas internacionais, esse intercâmbio é ainda mais interessante e combinado com uma viagem paga pelos organizadores. Alguns locais onde recentemente tivemos olimpíadas internacionais são Índia, Romênia, Coreia, Cuba, Uruguai, Brasil, entre outros.

O que objetiva-se com tais olimpíadas?[1]

> (i) descobrir e estimular talentos para o estudo da Matemática; (ii) contribuir na melhoria do ensino da Matemática em todos os níveis; (iii) aumentar a integração entre as universidades e as escolas; (iv) favorecer o aumento das relações entre alunos e professores, em escala nacional e internacional.

Toda Olimpíada de Matemática delimita o universo dos alunos que dela podem participar, sendo que essa delimitação pode ocorrer nos mais diversos âmbitos:

1. olimpíada local, restrita ao âmbito de uma certa escola;
2. olimpíada regional, aberta a alunos de uma dada região, como uma cidade, um estado;
3. olimpíada nacional, como é o caso da Olimpíada Brasileira de Matemática, organizada pela Sociedade Brasileira de Matemática e aberta a alunos do ensino primário, secundário e universitário brasileiro;
4. olimpíada internacional, como é o caso da Olimpíada Mundial de Matemática.

[1] http://www.mat.ufrgs.br/ portosil/olimpa1.htm

A ideia envolvida pode ser assim resumida: quanto menor for o âmbito de uma olimpíada menor será o nível de dificuldade de suas provas, mas maior a oportunidade de participação. Aqui no Brasil, já foi montada toda uma estrutura de organização que viabiliza ao aluno participar desde olimpíadas locais a olimpíadas internacionais.

A Olimpíada de Matemática é uma competição inspirada nos jogos olímpicos, que por sua vez são inspirados nos festivais esportivos que os gregos realizavam na antiga Grécia, em honra ao deus Zeus e outros deuses que habitavam o Olimpo.

Os festivais esportivos, ou competições entendidas como Olimpíadas de Matemática tinham como principais objetivos: induzir nos jovens o gosto e o prazer de estudar Matemática, estimular o ensino e aprendizagem da Matemática no Ensino Fundamental e no Ensino Médio e, por último, disponibilizar aos estudantes e professores uma coleção de problemas estimulantes e desafiadores.

A Olimpíada de Matemática é uma disputa entre os jovens, de caráter intelectual, um torneio onde as armas dos participantes são inteligência, criatividade, imaginação e disciplina mental. Na Olimpíada de Matemática, os estudantes concorrem experimentando o prazer de resolver problemas intrigantes. Este tipo de atividade intelectual, que valoriza a competência e o saber, é uma demonstração de civilidade e avanço cultural. A história da humanidade comprova que as sociedades mais desenvolvidas têm cultivado esse sentimento de respeito pelas vitórias do espírito. Importante registrar, a realização de Olimpíadas de Matemática no mundo é um acontecimento que data do século dezenove.

A primeira Olimpíada de Matemática ocorreu no Leste Europeu, mais precisamente na Hungria, em 1894, em homenagem ao Ministro da Educação da Hungria, Jósef Kurschák, professor de Matemática, membro da Academia de Ciências da Hungria e do Instituto Politécnico da Universidade de Budapeste. Essa ideia salutar foi disseminada pelo resto da Europa e para todo o mundo.

Figura 3.1: Jósef Kurschák

3.1 Olimpíadas de Matemática no Brasil

Vamos evidenciar duas Olimpíadas de Matemática Nacionais por ordem de criação: Olimpíada Brasileira de Matemática (OBM) e a Olimpíada Brasileira de Matemática das

Escolas Públicas (OBMEP); regionalmente, vamos destacar a Olimpíada Campinense de Matemática (OCM).

3.1.1 Olimpíada Brasileira de Matemática - OBM

A Olimpíada Brasileira de Matemática (OBM) é uma competição dedicada aos alunos brasileiros ou de escolas e universidades brasileiras das redes pública e privada desde o 6º ano do ensino fundamental até estudantes universitários em nível de graduação.

A Sociedade Brasileira de Matemática (SBM) organizou em 1979 a 1ª Olimpíada Brasileira de Matemática (OBM). Ao longo destes anos, a OBM passou por diversas mudanças em seu formato (Tabela 3.1), mantendo a ideia central que é a de estimular o estudo da Matemática pelos alunos, desenvolver e aperfeiçoar a capacitação dos professores, influenciar na melhoria do ensino, além de descobrir jovens talentos.

A OBM realiza-se anualmente em quatro níveis, de acordo com a escolaridade do aluno:

> **Nível 1** - para alunos matriculados nos 6º e 7º anos do ensino fundamental quando da realização da primeira fase da OBM.
>
> **Nível 2** - para alunos matriculados nos 8º e 9º anos do ensino fundamental quando da realização da primeira fase da OBM ou que, tendo concluído o ensino fundamental menos de um ano antes, não tenham ingressado no ensino médio até a data da realização da primeira fase da OBM.
>
> **Nível 3** - para alunos matriculados em qualquer série do ensino médio quando da realização da primeira fase da OBM ou que, tendo concluído o ensino médio menos de um ano antes, não tenham ingressado em curso de nível superior até a data de realização da primeira fase da OBM.
>
> **Nível Universitário** - para alunos que ainda não tenham concluído o curso superior (normalmente estudantes universitários em nível de graduação, podendo ser estudantes de qualquer curso e qualquer período), (OBM 2017).

Ano	Alteração
1979	1ª Olimpíada Brasileira de Matemática
1991	**Dois níveis:** **Júnior:** para alunos completando no máximo 15 anos em 1991. **Sênior:** para alunos cursando o ensino médio.
1992	**Duas fases:** **Primeira:** prova com 25 questões de múltipla escolha. **Segunda:** dois dias com 3 problemas em cada dia. **O nível Júnior** passa a ser para alunos cursando até a 9º ano.
1993	A 2ª fase do nível Júnior volta a ser realizada em um dia, com 5 problemas.
1995	O nível Júnior volta a ser para estudantes de até 15 anos.
1998	**Três níveis:** I: para alunos do 6º e 7º ano. II: para alunos do 8º e 9º ano. II: para alunos do Ensino Médio. **Três fases:** **Primeira:** múltipla escolha com 20 ou 25 questões. **Segunda:** prova aberta com 6 questões. **Terceira:** 5 questões (níveis I e II) e 6 questões no nível III (em dois dias). Realização das provas das duas primeiras fases nas Escolas cadastradas.
1999	As provas do nível II passam a ser realizadas em dois dias na fase final.
2011	É criado o nível Universitário, com duas fases.

Tabela 3.1: Evolução da Olimpíada Brasileira de Matemática - OBM

A partir da edição de 2017, a OBM passa a ser integrada juntamente com a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) com o objetivo de racionalizar a utilização dos recursos financeiros e humanos, bem como tornar mais eficientes os esforços pela divulgação e estímulo da Matemática no Brasil. A OBMEP, até o ano de 2016, contemplava apenas os alunos da rede pública mas, com a integração ocorrida em 2017, passou-se a contar, também, com a participação de discentes de instituições de ensino privadas.

São objetivos da OBM:

> (i) Interferir decisivamente na melhoria do ensino de Matemática em nosso país estimulando alunos e professores a um desenvolvimento maior propiciado pelas condições que atualmente podemos oferecer: a realização da OBM;
> (ii) Descobrir jovens com talento matemático excepcional, e colocá-los em contato com matemáticos profissionais e instituições de pesquisa de alto nível, propiciando condições favoráveis para a formação e o desenvolvimento de uma carreira de pesquisa;
> (iii) Selecionar os estudantes que representarão o Brasil em olimpíadas internacionais de Matemática a partir do seu desempenho na OBM, realizando seu devido treinamento;
> (iv) Apoiar as competições regionais em todo o Brasil;
> (v) Organizar as diversas competições internacionais de Matemática, quando realizadas no Brasil, (OBM 2017).

3.1.2 Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP

Pensando na melhoria do ensino de matemática nas escolas públicas de todo o País, o MEC, juntamente com a SBM e o Instituto de Matemática Pura e Aplicada (IMPA) estão promovendo e organizando, desde 2005, a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), que com cerca de 19 milhões de participantes a cada ano. Isto faz dela a maior Olimpíada de Matemática do mundo. A cada ano são premiados inúmeros alunos de diferentes estados, bem como professores e escolas. A OBMEP vem criando um ambiente estimulante para o estudo da Matemática entre alunos e professores de Escolas públicas em todo o Brasil.

Voltada para o ensino público, nos anos finais do ensino fundamental e ensino médio, a OBMEP tem o compromisso de afirmar a excelência como valor maior do ensino da matemática, além de mostrar a importância da disciplina para o futuro dos alunos e, consequentemente, para o desenvolvimento do país.

A OBMEP é destinada aos alunos do 6º ao 9º ano do Ensino Fundamental e aos alunos do Ensino Médio das Escolas públicas nas esferas municipais, estaduais e federais, sendo realizada em três níveis: no Nível 1 avaliam os alunos do 6º e 7º anos do Ensino Fundamental; no Nível 2 os alunos do 8º e 9º anos também do Ensino Fundamental e no Nível 3 os alunos da 1ª, 2ª e 3ª séries do Ensino Médio. Os alunos da (EJA) do 6º ou 7º ano do ensino fundamental deverão ser inscritos para as provas do Nível 1, os do 8º ou 9º ano, para as provas do Nível 2 e os do ensino médio, para as provas do Nível 3.

As provas dos Níveis 1, 2 e 3 são compostas de duas fases: participam da primeira fase todos os alunos da escola, os quais são inscritos pela própria escola de forma online para participarem da OBMEP, ficando aptos a segunda fase, cerca de 5% dos alunos inscritos pela escola em cada nível. Cabe a cada escola, por meio de um responsável, que, no geral, é o professor de matemática da própria escola, selecionar os alunos com melhor desempenho na primeira fase, classificando-os a participar da segunda fase; o responsável também deve fixar

previamente critérios de desempate a serem aplicados, se necessário, de modo a não exceder sua cota em cada nível.

A OBMEP premia os alunos com medalhas de ouro, de prata ou de bronze e certificados de menção honrosa, além de Bolsas de Iniciação Científica Júnior do CNPq. Os professores responsáveis pela organização das escolas públicas também são premiados com certificados, tablets e assinatura da Revista do Professor de Matemática (RPM). As escolas públicas são premiadas com kits de material didático e troféus. Os municípios são premiados com troféus. Todas essas premiações seguem critérios vinculados à premiação e pontos obtidos pelos alunos, descritos no Regulamento da OBMEP.

Vale frisar que na 1ª edição, foram 10.520.831 inscritos, 30.031 escolas, contemplando $93,5\%$ dos municípios brasileiros. Passados 12 anos, em sua 13ª edição e com 18.240.497 de alunos inscritos, 53.231 escolas e $99,57\%$ dos municípios participaram da OBMEP e continuam participando em grande número da OBMEP, sendo hoje, considerada a maior competição de Matemática do mundo.

Em 2016, foram premiados 48.984 alunos com medalhas e menções honrosas. Dessas premiações, 461 foram para alunos da Paraíba, com 6 medalhas de ouro, 8 medalhas de prata, 61 medalhas de bronze e 386 menções honrosas.

De forma contextualizada, as questões propostas na OBMEP trazem em seus enunciados questões-problema desafiadores, relacionadas a contextos reais e que ainda permitem que os alunos trabalhem com informações, discutam, interpretem e desenvolvam raciocínios próprios para chegarem à solução do problema proposto.

Em linhas gerais, os objetivos principais da Olimpíada Brasileira de Matemática das Escolas Públicas são:

> (i) Estimular e promover o estudo da Matemática entre alunos das escolas públicas;
>
> (ii) Contribuir para a melhoria da qualidade da Educação Básica;
>
> (iii) Identificar jovens talentos e incentivar seu ingresso nas áreas científicas e tecnológicas;
>
> (iv) Incentivar o aperfeiçoamento dos professores das escolas públicas, contribuindo para a sua valorização profissional;
>
> (v) Contribuir para a integração das escolas públicas com as universidades públicas, os institutos de pesquisa e as sociedades científicas;
>
> (vi) Promover a inclusão social por meio da difusão do conhecimento, (OBMEP 2017).

3.1.3 Olimpíada Campinense de Matemática - OCM

Localmente, a Olimpíada Campinense de Matemática (OCM) é uma atividade de extensão realizada pela Unidade Acadêmica de Matemática da Universidade Federal de Campina Grande, Campus Campina Grande, desde 1983. Portanto, já tem maioridade e uma

longa história que vem ao encontro dos objetivos que fundamentam a filosofia de olimpíadas culturais, na medida em que constitui um meio efetivo de detectar e estimular estudantes para estudos da Matemática, e prepará-los para competições nacionais e internacionais mediante uma competitividade saudável.

A OCM, no decorrer desse tempo, sofreu várias mudanças. Nos primeiros anos, era aplicada apenas para alunos do ensino médio. No início dos anos 90, foi também estendida para estudantes dos 8º e 9º anos. Só a partir de 1998, a OCM passou a ser realizada para alunos do ensino fundamental (a partir do 6ª ano), além do ensino médio. Nos últimos cinco anos, mais de 10 mil estudantes de mais de 60 escolas de Campina Grande e cidades circunvizinhas foram inscritos para participar da Olimpíada Campinense de Matemática.

A OCM leva no seu nome Olimpíada Campinense de Matemática Professor José Viera Alves, uma homenagem a um de seus fundadores professor José Vieira Alves do Departamento de Matemática do Centro de Ciências e Tecnologia, Campus Campina Grande, hoje professor aposentado.

Figura 3.2: José Vieira Alves

3.2 Olimpíadas de Matemática Internacionais

Abordaremos apenas quatro Olimpíadas de Matemática Internacionais: Olimpíada Internacional de Matemática (IMO), Ibero-Americana de Matemática, Cone Sul e a Olimpíada de Maio, as quais o Brasil vem marcando presença e se destacando com a conquista de várias medalhas.

3.2.1 Olimpíada Internacional de Matemática - IMO

A Olimpíada Internacional de Matemática (IMO) é a maior, mais antiga e prestigiada Olimpíada científica para alunos do ensino médio. A história da IMO data de 1959, quando a primeira edição foi realizada na Romênia com a participação de sete países: Romênia, Hungria, Bulgária, Polônia, Checoslováquia, Alemanha Oriental e URSS. Desde então, o evento é realizado anualmente (com exceção de 1980), sempre em um país diferente. Atualmente, mais de 100 países, dos 5 continentes, participam do evento. Cada país pode enviar uma

equipe de até seis alunos do ensino médio ou alunos que não tenham ingressado em uma universidade, ou instituição equivalente, na data de realização da Olimpíada, além de um líder da equipe, um vice-líder e observadores, se desejado.

Durante a IMO, os competidores devem resolver, individualmente, duas provas em dois dias consecutivos, com três problemas em cada dia. Cada problema vale 7 (sete) pontos. São concedidas medalhas de ouro, prata e bronze na proporção de $1 : 2 : 3$. De acordo com os resultados gerais, metade dos competidores recebem uma medalha. Para incentivar o maior número possível de alunos a resolverem problemas completos, são concedidos certificados de menção honrosa àqueles estudantes que não receberam medalha, mas obtiveram 7 (sete) pontos em pelo menos um problema.

O Brasil tem participado da IMO e obtido, por meio de seus jovens, diversas medalhas de ouro, prata e bronze. Em 2017, pela primeira vez, o Brasil sediou a IMO.

3.2.2 Olimpíada Ibero-Americana de Matemática

Existe também, desde 1985, patrocinada pela Organização dos Estados Ibero-Americanos para a Educação, Ciência e Cultura, a Olimpíada Ibero-Americana de Matemática. Nessa Olimpíada, o Brasil já conquistou, ao longo dos anos, medalhas de ouro, prata e bronze.

A primeira edição da Olimpíada Ibero-Americana de Matemática (OIM) foi realizada na Colômbia, sendo esta uma competição realizada anualmente para estudantes dos países da América Latina, Espanha e Portugal.

A equipe dos países é formada por quatro estudantes que não tenha completados 18 anos até 31 de dezembro do ano imediatamente anterior à celebração da olimpíada e não tenha participação em duas OIM's em anos anteriores. A equipe brasileira participa desta competição desde da primeira edição.

3.2.3 Olimpíada de Matemática do Cone Sul

Acontece também, anualmente, sempre em um país diferente, a Olimpíada de Matemática do Cone Sul, envolvendo estudantes do Brasil, Argentina, Bolívia, Chile, Equador, Paraguai, Peru e Uruguai. A primeira Olimpíada de Matemática do Cone Sul foi realizada em 1988 no Uruguai.

A equipe dos países é formada por quatro estudantes que não tenha completado 16 anos até 31 de dezembro do ano imediatamente anterior à celebração da olimpíada.

A equipe brasileira é formada por meio de um processo de seleção, em que todos os estudantes premiados com medalhas de ouro, prata, bronze e menções honrosas na OBM do ano anterior ao processo de seleção e os estudantes que tenham sido contemplados com medalhas em edições anteriores da OBM podem pedir para serem incluídos no processo de seleção, porém caberá à comissão de olimpíadas decidir se aceita o pedido ou não.

3.2.4 Olimpíada de Maio

O Brasil participa, também, das Olimpíadas de Maio, patrocinada pelo Centro Latino-Americano de Matemática e Informática (CLAMI) e pela Federação de Competições de Matemática.

É uma competição realizada para jovens alunos, disputada em dois níveis (Nível 1: para alunos até 13 anos e Nível 2: para alunos de até 15 anos), por países da América Latina, Espanha e Portugal. No Brasil, a Olimpíada de Maio é aplicada apenas àqueles alunos que tenham sido premiados na Olimpíada Brasileira de Matemática (OBM), com medalhas de ouro, prata, bronze e menções honrosas, ou tenham sido selecionados pelo coordenador regional. As provas dos alunos selecionados são enviadas à comissão organizadora na Argentina onde será dada a classificação final por país.

3.3 Guia de estudo sugerido para um bom desempenho nas Olimpíadas de Matemática

Muitas pessoas pensam que estudar para participar de uma Olimpíada de Matemática é avançar na matéria escolar, mas não é nada disso. Os problemas não exigem uma dose maior de conhecimento, e, sim, o despertar de um raciocínio e de muita criatividade. Em Olimpíadas de Matemática, são dados problemas de lógica onde o estudante deve chegar a uma das maneiras de resolver tais problemas. As sub-áreas [2] pelas quais é composta uma prova olímpica de Matemática são:

1. Álgebra:

   Desigualdades, Polinômios, Continuidade, Complexos, Produto notáveis, Equações e Sistemas, Girard, Recorrências, Funções definidas implicitamente, Indução, Máximos e Mínimos, Miscelânea sobre raízes, Somas de Newton, Diferenças finitas, Polinômios em $Z_{[x]}$, Irredutibilidade de polinômios, Números complexos e substituição trigonométrica.

2. Combinatória:

   (i) Estude casos pequenos: Busca de padrões, Obtenção de estruturas em contagens mais difíceis; Estude casos grandes: Comportamento assintótico de contagens.

   (ii) Contagem e Contagem Dupla: Bijeções, Probabilidades, Injeções, Sobrejeções, Obtenção de igualdades e desigualdades com contagem dupla, Recursões e estimativas utilizando recursões.

   (iii) Princípio da Casa dos Pombos: Formulação contínua, Teorema de Kronecker, Teorema de Ramsey.

[2] http://olimpiadascientificas.com/estudo/matematica/

(iv) Teoria dos Grafos: Indução (sempre reduzindo o casou para os anteriores, e não o contrário), Árvores, Algoritmo de Kruskai, Busca em profundidade, Busca em largura, Algoritmos de ordenação de conjuntos, Caminhos e circuitos eulerianos, Coloração de vértices em grafos, teorema das cinco cores, Teorema de Turán, Grafos planos $V - A + E = 2$, Teorema de Kuratowski, Grafos bipartidos (sem cíclos ímpares), Teorema dos casamentos, Max-Flow, Min-Cut.

(v) Geometria Combinatória: Conceitos: Diâmetro de um conjunto, conjunto convexo, Fecho convexo; Técnicas: casos extremos (problema de Silvester), Princípio da casa dos pombos (problemas envolvendo pinturas do plano, coberturas); Contagem (número de distâncias repetidas); Determinação de possíveis posições de um ponto indeterminado; escolha de uma direção adequada.

(vi) Invariantes: Determinação e construção de invariantes (paridade, restos, pinturas, funções), Semi-invariantes (determinação e construção), Invariante automático em recursões lineares homogêneas cujo polinômio característico é divisível por $x - 1$.

(vii) Indução: Como fazer a partir de casos pequenos; obtenção de algoritmos a partir da indução.

3. Geometria:

   Relações entre áreas, Congruência de triângulos, Ângulos na circunferência, Razão e Segmento, Quadriláteros notáveis, Relações métricas no triângulo, Pontos notáveis (Circuncentro e Ortocentro), Propriedades dos triângulos, Quadriláteros inscritíveis e circunscritíveis, Teorema de Ceva, Teorema de Menelaus, Potência de ponto e eixo radical, Caminhos mínimos, Quádruplas harmônicas, Transformações geométricas e Triângulo pedal.

4. Teoria dos Números:

   Divisibilidade, Equações diofantinas, A função parte inteira, Congruência, Algoritmo de Euclides, Ordem, Divisores, Mínimo múltiplo comum (MMC), Máximo divisor comum (MDC) e Números primos, Teorema do resto Chinês, Resíduos quadráticos, Ordem, Teorema fundamental da aritmética, Congruências e base, Teorema de Euler, Ordem e raízes primitivas, Congruências quadráticas, Anel de inteiros módulo n, Função de Euler, Teorema de Euler-Fermat, Congruências de ordem superior, Binomiais e primos, Polinômios ciclotômicos e primos, Sequências recorrentes e teste de Primalidade.

Como o conteúdo das Olimpíadas de Matemática é longo e sua intersecção com o conteúdo oficial da escola costuma ser pequeno, diversos alunos têm dúvidas sobre o que estudar, em verdade, não existe lista com os tópicos que são abordados na provas. Por isso,

transcrevemos acima orientações para alunos que pretendem se preparar para as Olimpíadas de Matemática.

Neste trabalho, vamos estudar alguns pontos referente ao item 4 citado anteriormente, Teoria do números.

Capítulo 4

Divisibilidade

Como a divisão de um número inteiro por outro nem sempre é possível, expressa-se essa possibilidade através da relação de divisibilidade.

Neste capítulo, vamos considerar o conceito de divisibilidade sobre o conjunto dos números inteiros e suas principais propriedades, que são extremamente importantes para nosso estudo.

4.1 Indução Matemática

Iniciamos este capítulo com a discussão de uma indispensável ferramenta na demonstração de muitos teoremas: O Princípio da Indução Matemática ou Princípio de Indução Finita (PIF). Enunciaremos, duas formas deste princípio e, também, o Princípio da Boa Ordenação (PBO).

4.1.1 Princípio da Boa Ordenação

O Princípio da Boa Ordenação considerado a seguir é seguramente uma das mais fortes ferramentas usadas em demonstrações matemáticas. Ele é a base para uma série de resultados sobre os números inteiros.

Definição 4.1 *Seja X um subconjunto não vazio de $\mathbb{Z}$. Dizemos que X é limitado inferiormente* [1] *quando existe um elemento $x_0 \in \mathbb{Z}$ tal que*

$$x_0 \leq x, \forall x \in X.$$

Axioma 4.1 ***(Princípio da Boa Ordenação - PBO)*** *Todo subconjunto não vazio e limitado inferiormente X de $\mathbb{Z}$ possui menor elemento.*

[1] Da mesma forma, definimos conjunto *limitado superiormente e elemento máximo (ou maior elemento)* de um conjunto.

Como todo subconjunto não vazio de $\mathbb{N}$ é limitado inferiormente, então para o conjunto dos números naturais, o PBO se reduz à afirmação: *todo subconjunto não vazio X de $\mathbb{N}$ possui um menor elemento.*

Um limitante inferior de um conjunto X pode ou não pertencer a X; contrário a isso, um elemento mínimo de X, por definição, pertence a X.

Proposição 4.1 *Nas condições do Axioma 4.1, o elemento mínimo de X é único.*

Demonstração: Se x_0 e y_0 são elementos mínimos de X, então $x_0 \leq y_0$ e $y_0 \leq x_0$. Mas isto em $\mathbb{Z}$ implica $x_0 = y_0$, pois a relação " $\leq$ " é antissimétrica. ■

Indicaremos o elemento mínimo x_0 de X por

$$x_0 = minX.$$

Proposição 4.2 *Seja a um número inteiro. Se $a > 0$, então $a \geq 1$.*

Demonstração: Provemos por absurdo. Suponhamos que exista $m \in \mathbb{Z}$ tal que $0 < m < 1$. Desse modo,

$$X = \{m \in \mathbb{Z} : 0 < m < 1\}$$

é não vazio e limitado inferiormente e, pelo PBO, possui um menor elemento x_0. Como $x_0 \in X$, segue que

$$0 < x_0^2 < x_0 < 1,$$

ou seja, $0 < {x_0}^2 < 1$, o que implica ${x_0}^2 \in X$, com ${x_0}^2 < x_0$, contrariando a minimalidade de x_0. ■

Corolário 4.3 *Sejam a e b inteiros quaisquer. Se $a > b$, então $a \geq b + 1$.*

Demonstração: Como $a - b > 0$, então pela proposição anterior, $a - b \geq 1$, ou seja, $a \geq b + 1$. ■

Proposição 4.4 ***(Propriedade Arquimediana)*** *Se a e b são números naturais, então existe um número natural n tal que $na \geq b$.*

Demonstração: Vamos supor que a afirmação não seja verdadeira, de modo que para todo natural n, temos, $na < b$. Logo, o conjunto

$$S = \{b - na : n \in \mathbb{N}\}$$

é formado apenas por números naturais. Pelo PBO, S possui elemento mínimo, digamos $m = minS$. Como $m \in S$, existe $n_0 \in \mathbb{N}$ tal que $m = b - n_0 a$. Por outro lado, o elemento $m_1 = b - (n_0 + 1)a$ pertence a S, pois S contém todos os elementos dessa forma. Além disso,

$$m_1 = b - (n_0 + 1)a = b - n_0 a - a = m - a < m,$$

pois $a > 0$. Assim, $m_1 \in S$ e $m_1 < m$, o que contraria o fato de m ser o menor elemento de S. Isso conclui a demonstração. ■

4.1.2 Princípio de Indução Finita

No que segue, $P(n)$ é uma sentença aberta que depende da variável n sobre um subconjunto infinito e limitado inferiormente X de $\mathbb{Z}$, ou seja, uma sentença que contém n, de maneira que, toda vez que se substitui n por $a \in X$, obtêm-se uma sentença $P(a)$ que é, sem ambiguidade, verdadeira ou falsa.

Teorema 4.5 ***(Princípio de Indução Finita - 1ª Forma)*** *Seja $P(n)$ uma sentença em $\{n \in \mathbb{Z} : n \geq n_0\}$, em que $n_0 \in \mathbb{Z}$. Então, $P(n)$ é verdadeira para todo $n \geq n_0$, desde que $P(n)$ satisfaça as seguintes condições:*

(i) $P(n_0)$ é verdadeira.

(ii) Se $P(n)$ é verdadeira para $n \geq n_0$, então $P(n+1)$ também é verdadeira.

Demonstração: Consideremos o conjunto

$$X = \{n \in \mathbb{Z} : n \geq n_0 \ \ e \ \ P(n) \ \ falsa\}.$$

Desejamos mostrar que $X = \emptyset$. Suponhamos por absurdo que $X \neq \emptyset$. Como X é limitado inferiormente *(por n_0, por exemplo)*, então pelo PBO, existe $m_0 \in X$, elemento mínimo de X, tal que

$$m_0 \leq n, \ \ \forall n \in X$$

Como $m_0 \in X$, $m_0 \geq n_0$ e $P(m_0)$ é falsa então, $m_0 \neq n_0$, pois, por hipótese, $P(n_0)$ é verdadeira. Assim, $m_0 > n_0$ e, pelo Corolário 4.3, $m_0 - 1 \geq n_0$. Sendo $m_0 = minX$, segue que $m_0 - 1 \notin X$. Portanto, $P(m_0 - 1)$ é verdadeira, de modo que, pela condição (ii),

$$P(m_0 - 1 + 1) = P(m_0)$$

é verdade e, assim, $m_0 \notin X$, o que é uma contradição. Logo, $X = \emptyset$ e, portanto, $P(n)$ é verdadeira para todo $n \geq n_0$. ■

A condição (i) do Teorema 4.5 é chamada de *base da indução*, a qual consiste em verificar a validade de $P(n)$ para o valor de $n = n_0$, chamado *valor inicial*. Já a condição (ii) é chamada de *passo indutivo ou passo de indução*, cuja hipótese é chamada *hipótese de indução*. O passo indutivo consiste em mostrar a validade de $P(n+1)$, desde que $P(n)$ seja válida, com $n \geq n_0$. Satisfeitas as condições (i) e (ii), obtemos as seguintes implicações:

$$\begin{aligned} P(n_0)\ Verdadeira &\Rightarrow P(n_0+1)\ Verdadeira \\ &\Rightarrow P(n_0+2)\ Verdadeira \\ &\Rightarrow P(n_0+3)\ Verdadeira \\ &\vdots \end{aligned}$$

de maneira que $P(n)$ é verdadeira para todo número natural $n \geq n_0$.

Teorema 4.6 ***(Princípio de Indução Finita - 2ª Forma)*** *Seja $P(n)$ uma sentença em $\{n \in \mathbb{Z} : n \geq n_0\}$, em que $n_0 \in \mathbb{Z}$. Então, $P(n)$ é verdadeira para todo $n \geq n_0$, desde que $P(n)$ satisfaça as seguintes condições:*

(i) ***(Base da Indução)*** *$P(n_0)$ é verdadeira.*

(ii) ***(Passo Indutivo)*** *Se $P(k)$ é verdadeira para todo inteiro k tal que $n_0 \leq k \leq n$, então $P(n+1)$ é também verdadeira.*

Demonstração: A prova é análoga à da primeira forma. Tomemos o conjunto

$$X = \{n \in \mathbb{Z} : n \geq n_0 \ e\ P(n)\ falsa\}.$$

Queremos provar que $S = \emptyset$. Por absurdo, suponhamos que $S \notin \emptyset$. Como S é limitado inferiormente, segue do PBO que existe $m_0 \in S$ *(elemento mínimo de S)* tal que

$$m_0 \leq n,\ \forall n \in S.$$

Como $m_0 \in S$, então $m_0 \geq n_0$ e $P(m_0)$ é falsa. Logo, pela condição (i), $m_0 \notin n_0$. Sendo $m_0 = minS$, então $P(k)$ é verdadeira para todo $k \in \mathbb{Z}$ tal que $n_0 \leq k \leq m_0 - 1$. Desse modo, pela condição (ii), podemos concluir que $P(m_0)$ é verdadeira, o que é uma contradição. Por isso, $S = \emptyset$ e, por conseguinte, $P(n)$ é verdadeira para todo $n \geq n_0$. ■

Exemplo 4.1 Mostrar, usando indução finita, que

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2},\ \forall\, n\ \in\ \mathbb{N}.$$

Solução: Seja $P(n)$ a sentença sobre $\mathbb{N}$ dada por

$$P(n): 1+2+\cdots+n = \frac{n(n+1)}{2}.$$

É evidente que $P(n_0 = 1)$ é verdadeira (base de indução). Assim, por hipótese de indução, vamos supor que $P(k)$ seja verdadeira, com $k \geq 1$, e provemos que $P(k+1)$ também o é. Por hipótese,

$$1+2+\cdots+k = \frac{k(k+1)}{2}.$$

Somando $k+1$ a ambos os membros desta igualdade, obtemos

$$\begin{aligned} 1+2+\cdots+k+(k+1) = &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

o que prova que $P(k+1)$ é verdadeira. Portanto, pelo Princípio de Indução Finita, concluímos que $p(n)$ é verdadeira para todo $n \geq 1$. ▲

Exemplo 4.2 Mostrar que $1+n \leq 2^n$ para todo $n \geq 0$.

Solução: Consideremos

$$P(n): 1+n \leq 2^n, \ \ \forall\, n \geq 0.$$

Como $1+0 = 1 \leq 2^0$, temos que $P(0)$ é verdadeira. Suponhamos que $1+k \leq 2^k$, com $k \geq 0$. Multiplicando os membros de $1+k \leq 2^K$ por 2, obtemos

$$2+2k \leq 2^{k+1},$$

de modo que,

$$1+(k+1) = 2+k \leq 2+2k \leq 2^{k+1}.$$

Isso mostra que $P(k+1)$ é verdadeira e, portanto, $P(n)$ é verdadeira para todo $n \geq 0$. ▲

4.2 Tópicos Relativos a Divisibilidade

Dados dois números inteiros d e a, diremos que *d divide a* ou que d é um divisor de a ou ainda que a é um *múltiplo* de d, e escrevemos

$$d|a$$

se existir $q \in \mathbb{Z}$ com $a = qd$. Caso contrário, escrevemos $d \nmid a$. Por exemplo, temos que $-5|10$ mas $10 \nmid -5$.

Lema 4.7 *Sejam $a,b,c,d \in \mathbb{Z}$. Temos*

(i) Se $d|a$ e $d|b$, então $d|ax+by$ para qualquer combinação linear $ax+by$ de a e b com coeficientes $x,y \in \mathbb{Z}$.

(ii) *(Limitação)* Se $d|a$, então $a = 0$ ou $|d| \leq |a|$.

(iii) *(Transitividade)* Se $a|b$ e $b|c$, então $a|c$.

(iv) Se $a|b$ e $c|d$, então $ac|bd$.

Demonstração: (i) Se $d|a$ e $d|b$, então podemos escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax+by = d(q_1x+q_2y)$. Como $q_1x+q_2y \in \mathbb{Z}$, temos que $d|ax+by$.

(ii) Suponha que $d|a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d| \Rightarrow |a| \geq |d|$.

(iii) Se $a|b$ e $b|c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto, $a|c$.

(iv) Como $a|b$ e $c|d$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $d = cq_2$, logo $db = (ac)(q_1q_2)$ e portanto $ac|bd$. ■

Proposição 4.8 *Em $\mathbb{Z}$ valem as seguintes propriedades:*

(i) Os únicos divisores de 1 são 1 e -1;

(ii) Se $a|b$ e $b|a$, então $a = \pm b$.

Demonstração: (i) Se b é um divisor de 1, então pelo Lema 4.7 (ii), $|b| \leq 1$. Assim, $0 < |b| \leq 1$. Como não existe inteiro entre 0 e 1 *(Proposição 4.4)*, concluímos que $|b| = 1$, isto é, $b = \pm 1$.

(ii) Por hipótese, $a = q_1 b$ e $b = q_2 a$, com $q_1, q_2 \in \mathbb{Z}$. Desse modo,

$$a = (q_1 q_2)a,$$

ou seja, $q_1 q_2$=1 e, pelo item (i), $q_1 = \pm 1$, o que implica em $a = \pm b$. ■

4.2.1 Algoritmo da Divisão

Um dos fundamentos de muitos resultados da Teoria dos Números é certamente o Algoritmo da Divisão. [2] Uma das propriedades mais importantes dos números inteiros é a possibilidade de dividir um número por outro com resto pequeno. Essa é a chamada *Divisão Euclidiana ou Divisão com Resto*. Por exemplo, tomando os inteiros $a = 26$ e $b = 4$, então dividindo a por b, obtemos

$$26 = 4.6 + 2$$

De uma forma geral, temos:

Teorema 4.9 ***(Algoritmo da Divisão)*** *Sejam a e b inteiros, com $b > 0$. Então, existem únicos inteiros q e r tais que*

$$a = bq + r, \ \ com \ \ 0 \leq r < b.$$

Demonstração: Consideremos o conjunto

$$L = \{a - bq : q \in \mathbb{Z} \ \ e \ \ a - bq \geq 0\}.$$

Uma primeira coisa a ser verificada é que L é não vazio. De fato, desde que $b \geq 1$, então $|a|.|b| \geq |a|$. Logo,

$$a - (-|a|).b = a + |a|.b \geq a + |a| \geq 0.$$

Como $x = a - (-|a|).b$ é da forma $a - bq$, com $q = -|a|$. segue que $x \in L$. Agora, vamos mostrar a existência e unicidade dos inteiros q e r.

(Existência): Sendo L limitado inferiormente (por zero, por exemplo) e não vazio, pelo PBO L possui menor elemento, digamos $r = minL$. Como $r \in L$, então $r \geq 0$ e

$$r = a - bq, \ \ com \ \ q \in \mathbb{Z}.$$

Asseguramos que $r < b$. De fato, se isto não ocorre, então $r - b \geq 0$ e

$$r - b = a - bq - b = a - b(q + 1).$$

[2] Esse Algoritmo é destacado no Livro VII dos *Elementos* de Euclides em sua Proposição 2.

Portanto, $r-b \in L$ e $r-b < r$, o que contraria a minimalidade de r. Assim, $a = qb+r$, com $q \in \mathbb{Z}$ e $0 \leq r < b$, o que prova a existência dos inteiros q e r.

(Unicidade): Para a unicidade, consideremos $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = bq_1 + r_1, \ \ com \ \ 0 \leq r_1 < b.$$

Assim, $bq + r = bq_1 + r_1$, o que implica

$$r - r_1 = b(q_1 - q),$$

ou seja, $b|(r-r_1)$. Como $|r-r_1| < b$, segue que $r - r_1 = 0$, isto é, $r = r_1$.

Por isso, $q_1 = q$, uma vez que $b \neq 0$. ■

Uma versão mais geral do Algoritmo da Divisão é obtida quando substituímos a condição $b > 0$ por $b \neq 0$, de acordo com o seguinte:

Corolário 4.10 ***(Algoritmo da Divisão - Versão Geral)*** *Se a e b são inteiros, com $b \neq 0$, então, existem inteiros q e r tais que*

$$a = bq + r, \ \ com \ \ 0 \leq r < |b|.$$

Demonstração: É suficiente considerar o caso $b < 0$. O teorema anterior nos mostra que existem, únicos inteiros q e r tais que

$$a = |b|q_1 + r, \ \ com \ \ 0 \leq r < |b|.$$

Como $|b| = -b$, então

$$a = |b|q_1 + r = b(-q_1) + r,$$

de maneira que, tomando $q = -q_1$, obtemos

$$a = bq + r, \ \ com \ \ 0 \leq r < |b|.$$

■

Os inteiros q e r dados no Corolário 4.10 são chamados de *quociente* e *resto* da Divisão Euclidiana de a por b, respectivamente. Às vezes, r também é dito o *resto de a módulo b*. Quando $b > 0$, r é indicado por $r \equiv a(mod\ b)$.

4.2.2 Sistema de Numeração

Os números naturais foram representados ao longo da história de vários modos distintos. O modo universalmente utilizado na atualidade é a representação decimal posicional. Esse sistema é diferente do sistema sexagesimal utilizado pelos babilônios há cerca de 1700 anos antes de Cristo, foi desenvolvido na China e na Índia. No sistema atual, todo número natural é representado por uma sequência formada pelos algarismos

$$0,1,2,3,4,5,6,7,8,9.$$

Por serem 10 algarismos, o sistema é chamado de decimal. O sistema é também dito posicional, pois cada algarismo, além de seu valor intrínseco, possui um peso que lhe é atribuído em função de sua posição dentro da sequência. Esse peso é uma potência de 10 e varia do seguinte modo: O algarismo da extrema direita tem peso $10^0 = 1$; o seguinte, sempre da direita para a esquerda, tem peso $10^1 = 10$; o seguinte, $10^2 = 100$; o próximo $10^3 = 1000$ e assim por diante.

Deste modo, o número $a = 1458$ no sistema decimal representa o número

$$a = 1.10^3 + 4.10^2 + 5.10^1 + 8.10^0 = 1.10^3 + 4.10^2 + 5.10 + 8.$$

Os zeros à esquerda em um número são irrelevantes, por exemplo,

$$b = 0231 = 0.10^3 + 2.10^2 + 3.10 + 1 = 2.10^2 + 3.10 + 1 = 231.$$

Cada algarismo de um número possui uma *ordem*, contada da direita para a esquerda. Assim, no caso do exemplo acima, o 8 é de primeira ordem, o 5 de segunda ordem, o 4 de terceira ordem e o 1 de quarta ordem.

Cada três ordens, também contadas da direita para a esquerda, constituem uma *classe*. As classes são usualmente separadas por um ponto. A seguir, damos os nomes das primeiras classes e ordens:

(i) **classe das unidades** *(unidades 1^a ordem, dezenas 2^a ordem, centenas 3^a ordem)*;

(ii) **classe do milhar** (*unidades de milhar 4^a ordem, dezenas do milhar, 5^a ordem; centenas do milhar 6^a ordem)*;

(iii) **classe do milhão** (*unidades de milhão, 7^a ordem; dezenas de milhão, 8^a ordem; centena de milhão 9^a ordem).*

De modo geral, um número $a = r_n r_{n-1} ... r_1 r_0$ no sistema decimal é escrito de forma única como uma soma finita, na qual cada parcela é um múltiplo de uma potência de 10. Mas precisamente,

$$a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$$

Os sistemas de numeração posicional baseiam-se no teorema a seguir, que é uma aplicação da *Divisão Euclidiana*.

Teorema 4.11 *Seja b um inteiro, com $b > 1$. Então, todo inteiro positivo a pode ser escrito de modo único na forma*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0,$$

em que $n \geq 0$, $r_n \neq 0$, e para cada i, com $0 \leq i \leq n$, temos que $0 \leq r_i < b$.

Demonstração: A prova consiste em mostrar a existência e unicidade dos números r_i's, $i = 0, 1, \cdots, n$. Isso será feito usando divisões sucessivas.

(Existência): Dividindo a por b, obtemos pelo Algoritmo da Divisão que

$$a = bq_0 + r_0, \qquad 0 \leq r_0 < b.$$

Dividindo q_0 por b,

$$q_0 = bq_1 + r_1, \qquad 0 \leq r_1 < b.$$

Se $q_1 \geq b$, então dividindo q_1 por b,

$$q_1 = bq_2 + r_2, \qquad 0 \leq r_2 < b.$$

Repetindo o processo e levando em consideração que cada quociente q_i é não negativo e $q_{i+1} < q_i$ para $i \geq 1$, devemos obter necessariamente um quociente igual a zero, digamos $q_n = 0$. Desse modo,

$$q_{n-2} = bq_{n-1} + r_{n-1},$$

com $0 \leq r_{n-1} < b$ e $q_{n-1} = bq_n + r_n = r_n$.
Agora, substituindo os valores dos quocientes q_i's de forma sucessiva, começando com q_0, obtemos que

$$\begin{aligned}
a = bq_0 + r_0 &= b(bq_1 + r_1) + r_0 \\
&= b^2 q_1 + br_1 + r_0 \\
&= b^2(bq_2 + r_2) + br_1 + r_0 \\
&= b^3 q_2 + b^2 r_2 + br_1 + r_0 \\
&\vdots \\
&= b^{n-1}(bq_{n-1} + r_{n-1}) + b^{n-2} r_{n-2} + \cdots + b^2 r_2 + br_1 + r_0 \\
&= b^n bq_{n-1} + b^{n-1} r_{n-1} + b^{n-2} r_{n-2} + \cdots + b^2 r_2 + br_1 + r_0.
\end{aligned}$$

Mas, como $q_{n-1} = r_n$, temos

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0.$$

Isso prova a existência da expressão de a sob as hipóteses estabelecidas.

(Unicidade): Mostremos inicialmente que, nas condições anteriores, $b_n \leq a < b^{n+1}$. Com efeito, como $1 \leq r_n$, então $b^n \leq r_n b^n \leq a$. Por outro lado, como $r_i < b$, segue que $r_i \leq b-1$. Logo,

$$\begin{aligned} a &= r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0 \\ &\leq (b-1)b^n + (b-1)b^{n-1} + \cdots + (b-1)b + (b-1) \\ &= b^{n+1} - 1 \\ &< b^{n+1}. \end{aligned}$$

Logo, $b^n \leq a < b^{n+1}$. Agora, suponhamos que

$$a = s_m b^m + s_{m-1} b^{m-1} + \cdots + s_1 b + s_0,$$

em que $0 \leq s_i < b$ para $i = 0, 1, ..., m$. Nestas condições, $n = m$. De fato, se $m < n$, então $m+1 \leq n$, de modo que, $b^{m+1} \leq b^n \leq a$, o que não é possível, pois $a < b^{m+1}$. Da mesma forma, não se pode ter $n < m$. Portanto, $m = n$. Desse modo,

$$r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0 = s_n b^n + s_{n-1} b^{n-1} + \cdots + s_1 b + s_0.$$

Assim,

$$b(r_n b^{n-1} + \cdots + r_2 b + r_1) + r_0 = b(s_n b^{n-1} + \cdots + s_2 b + s_1) + s_0. \tag{4.1}$$

Como $0 \leq r_i < b$ e $0 \leq s_i < b$, então da unicidade assegurada pelo Algoritmo da Divisão para o quociente e o resto, concluímos de (4.1) que $r_0 = s_0$. Logo,

$$r_n b^{n-1} + r_{n-1} 1 b^{n-2} + \cdots + r_2 b + r_1 = s_n b^{n-1} + s_{n-1} b^{n-2} + \cdots + s_2 b + s_1.$$

Da mesma forma,

$$b(r_n b^{n-2} + r_{n-1} b^{n-3} + \cdots + r_2) + r_1 = b(s_n b^{n-2} + s_{n-1} b^{n-3} + \cdots + s_2) + s_1,$$

e pelo mesmo motivo, $r_1 = s_1$ e

$$r_n b^{n-2} + r_{n-1} b^{n-3} + \cdots + r_2 = s_n b^{n-2} + s_{n-1} b^{n-3} + \cdots + s_2.$$

Continuando estes processo, obtemos que $r_i = s_i$, para $i = 1, ..., n$. ■

Definição 4.2 *Nas condições do teorema anterior, a expansão*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$$

é chamada ***expansão de*** *a* ***na base*** *b ou* ***expansão*** *b****-ádica*** *de a, a qual indicaremos por*

$$[r_n r_{n-1} \ldots r_1 r_0]_b.$$

4.2.3 Alguns Critérios de Divisibilidade

Vamos considerar alguns critérios de divisibilidade considerando a representação decimal de um dado número natural. Conforme provamos anteriormente, todo número natural a pode ser escrito de maneira única da seguinte forma.

$$a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0, \tag{4.2}$$

em que $n \geq 0$, $r_n \neq 0$, e para cada i, com $0 \leq i \leq n$, $0 \leq r_i < 10$.

(i) **Divisibilidade por** 2**,** 5 **e** 10

Os critérios de divisibilidade por 2, 5 e 10 são obtidos de forma direta. De fato, como

$$r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0,$$

é uma soma na qual todas as n primeiras parcelas são múltiplos de 2, 5 e 10 simultaneamente, segue de (4.2) que

$$2|a \ \Leftrightarrow \ 2|r_0 \ \Leftrightarrow \ r_0 \text{ é par}$$

ou seja, 2 divide a se, e somente se, $r_0 = 0, 2, 4, 6$ ou 8. Em outras palavras, *um número inteiro qualquer a é divisível por* 2 *se, e somente se, seu último dígito ou dígito das unidades for par*.

Por exemplo, $a = 545898$ é divisível por 2, já $b = 434565$ não o é.

Na divisibilidade por 5, *um número inteiro qualquer a é divisível por* 5 *se, e somente se, seu último dígito for* 0 *ou* 5. De fato,

$$5|a \ \Leftrightarrow \ 5|r_0 \ \Leftrightarrow \ r_0 = 0 \ \ ou \ \ r_0 = 5.$$

Assim, $a = 25590$ e $b = 75425$ são divisíveis por 5, já $c = 14467$ e $d = 5463$ não são.

No caso da divisibilidade por 10, *um número inteiro qualquer a é divisível por* 10 *se, e somente se, seu último dígito for* 0. Com efeito,

$$10|a \Leftrightarrow 10|r_0 \Leftrightarrow r_0 = 0.$$

pois, r_0 é o único múltiplo de 10.

(ii) **Divisibilidade por** 3 **e** 9

Os critérios de divisibilidade por 3 e 9 são os mesmos. Vamos começar mostrando por indução sobre n que

$$9|10^n - 1, \ \ \forall n \geq 0. \tag{4.3}$$

Como, $9|10^0 - 1 = 0$, então o resultado é válido para $n = 0$. Supondo $10^n - 1 = 9k$, ou seja, $10^n = 9k + 1$, então

$$\begin{aligned} 10^{n+1} - 1 = 10^n.10 - 1 &= (9k+1).10 - 1 \\ &= 90k + 9 \\ &= 9(10k+1), \end{aligned}$$

isto é, $9|10^{n+1} - 1$. Portanto, $9|10^n - 1$ para todo $n \geq 0$.

Agora, considerando $a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$, temos

$$a - (r_n + r_{n-1} + \cdots + r_1 + r_0) = r_n(10^n - 1) + r_{n-1}(10^{n-1} - 1) + \cdots + r_1(10 - 1).$$

De acordo com (4.3), os termos à direita da última igualdade são sempre divisível por 9. Logo,

$$a - (r_n + r_{n-1} + \cdots + r_1 + r_0) = 9k, \text{ com } k \in \mathbb{Z}.$$

Assim, se 9 divide a, então 9 divide $r_n + r_{n-1} + \cdots + r_1 + r_0$ (soma dos dígitos de a). Reciprocamente, se 9 divide $r_n + r_{n-1} + \cdots + r_1 + r_0$, então 9 divide a. Portanto, *um número inteiro qualquer a é divisível por* 9 *se, e somente se, a soma de seus dígitos é divisível por* 9.

Como 3 divide 9, então $3|10^n - 1$, de modo que o critério por 3 é o mesmo critério de 9. Ou seja, *um número inteiro a é divisível por* 3 *se, e somente se, a soma de seus dígitos é divisível por* 3.

Desse modo, $a = 345$ e $b = 34125$ são divisíveis por 3, pois

$$3 + 4 + 5 = 12 = 3.4 \ \text{ e } \ 3 + 4 + 1 + 2 + 5 = 15 = 3.5$$

Já os números $c = 1234$ e $d = 2063$ não são, pois $1 + 2 + 3 + 4 = 10$ e $2 + 0 + 6 + 3 = 11$. Similarmente, $a = 4302$ e $b = 8109$ são divisíveis por 9, mas $c = 2341$ e $d = 11306$ não são.

(iii) **Divisibilidade por** 4

Podemos escrever o número $a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$ da seguinte forma:

$$a = 100k + r_1 r_0,$$

pois $r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_2 10^2$ é divisível por $100 = 4.25$. Sendo assim, para estudar a divisibilidade por 4, basta analisar o número $r_1 r_0$, que é formado pelos dígitos das dezenas com o das unidades. Resumindo, *um número inteiro a é divisível por* 4 *se, e somente se, o número formado pelos dígitos das dezenas e das unidades é divisível por* 4.

Por exemplo, o número $a = 671032$ é divisível por 4, pois 32 é múltiplo de 4. Por outro lado, como 23 não é múltiplo de 4, então $b = 456823$ não é divisível por 4.

(vi) **Divisibilidade por** 7

O critério de divisibilidade por 7 é obtido com um pouco mais de detalhes. Consideremos

$$a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$$

ou melhor,

$$a = 10k + r_0,$$

pois $r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10$ é múltiplo de 10, com $k = r_n r_{n-1}...r_2 r_1$ (o número formado pelos dígitos de a, exceto o dígito das unidade).

Vamos mostrar que

$$7|a \;\Leftrightarrow\; 7|k - 2r_0.$$

De fato, se 7 divide a, então existe um inteiro m tal que $a = 7m$. Logo, como $r_0 = a - 10k$,

$$\begin{aligned} k - 2r_0 = k - 2(a - 10k) &= k - 2(7m - 10k) \\ &= k - 14m + 20k \\ &= 7(3k - 2m), \end{aligned}$$

isto é, 7 divide $k - 2r_0$. Reciprocamente, se $7|k - 2r_0$, então $k - 2r_0 = 7\alpha$, com $\alpha \in \mathbb{Z}$, ou seja, $k = 7\alpha + 2r_0$. Desse modo,

$$a = 10k + r_0 = 10(7\alpha + 2r_0) + r_0 = 7(10\alpha + 3r_0),$$

logo, 7 divide a. Isso conclui a prova. Assim, *um número inteiro qualquer a é divisível por 7 quando a diferença entre as suas dezenas e o dobro do valor do algarismo das unidades é*

divisível por 7.

Verifiquemos se o número $a = 13104$ é divisível por 7. Neste caso, temos que $k = 1310$ e $r_0 = 4$. Logo,

$$k - 2r_0 = 1310 - 2.4 = 1302.$$

O número 1320 é menor do que 13104, mas ainda não é "fácil" identificar de imediato sua divisibilidade por 7. Por isso, vamos aplicar o mesmo processo ao número 1302. Para este, temos $k = 130$ e $r_0 = 2$, de modo que

$$k - 2r_0 = 130 - 2.2 = 126.$$

Mais uma vez, aplicando o processo com $k = 12$ e $r_0 = 6$,

$$12 - 2.6 = 0.$$

Como $7|0$, então $7|126$, implicando que $7|1302$ e, por conseguinte, $7|13104$. Analisemos agora o número $a = 10890$. De forma sucessiva, temos

$$\begin{aligned} 1089 - 2.0 &= 1089, \\ 108 - 2.9 &= 90, \\ 9 - 2.0 &= 9. \end{aligned}$$

Como $7 \nmid 9$, então $7 \nmid 10890$.

(vi) **Divisibilidade por** 11

Vamos concluir considerando o critério de divisibilidade por 11. Em primeiro lugar, provemos por indução que

$$11|10^{2k} - 1, \ \ \forall k \in \mathbb{N}.$$

Para $k = 1$, temos que $10^2 - 1 = 99 = 11.9$. Por hipótese de indução, suponhamos que $10^{2k} - 1 = 11\lambda$, ou seja, $10^{2k} = 11\lambda + 1$. Logo,

$$\begin{aligned} 10^{2(k+1)} - 1 = 10^{2k}.10^2 - 1 &= (11\lambda + 1).10^2 - 1 \\ &= 11.100\lambda + 99 \\ &= 11.(100\lambda + 9). \end{aligned}$$

Portanto, 11 divide $10^{2(k+1)} - 1$, o que mostra o resultado. Com isso,

$$10^{2k+1} + 1 = 11\lambda$$

para algum $\lambda \in \mathbb{N}$. Em resumo, $11|(10^n-1)$ se n é par, e $11|(10^n+1)$ se n é ímpar.

Com esses resultados em mãos, já podemos analisar a divisibilidade de um número natural a por 11. De fato, consideremos

$$a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0,$$

em que

$$10^{2k_i} = 1 + 11\lambda_i, \text{ com } k_i = i \text{ para } i = 1, 2, ...$$

e

$$10^{2k_i+1} = -1 + 11\alpha_i, \text{ com } k_i = i \text{ para } i = 0, 1, ...$$

Agrupando as parcelas de índices pares e ímpares separadamente, obtemos

$$a = (r_0 + r_2 10^2 + r_4 10^4 + \cdots) + (r_1 10 + r_3 10^3 + r_5 10^5 + \cdots).$$

Temos,

$$\begin{aligned} r_0 + r_2 10^2 + r_4 10^4 + \cdots &= [r_0 + r_2(1 + 11\lambda_1) + r_4(1 + 11\lambda_2) + \cdots] \\ &= (r_0 + r_2 + r_4 + \cdots) + 11\lambda, \end{aligned}$$

com $\lambda \in \mathbb{N}$. Da mesma forma,

$$r_1 10 + r_3 10^3 + r_5 10^5 + \cdots = -(r_1 + r_3 + r_5 + \cdots) + 11\alpha,$$

para algum $\alpha \in \mathbb{Z}$. Portanto,

$$a = (r_0 + r_2 + r_4 + r_6 + \cdots) - (r_1 + r_3 + r_5 + r_7 + \cdots) + 11\beta,$$

em que $\beta = \lambda + \alpha$. Pondo

$$S_p = r_0 + r_2 + r_4 + r_6 + \cdots \text{ (a soma dos dígitos de índice par)}$$

e

$$S_I = r_1 + r_3 + r_5 + r_7 + \cdots \text{ (a soma dos dígitos de índice ímpar),}$$

concluímos que: *um número inteiro qualquer a é divisível por* 11 *se, e somente se,* $S_p - S_I$ *é divisível por* 11.

Por exemplo, para o número $a = 1125795$, temos

$$\begin{aligned} r_0 = 5,\ r_2 = 7,\ r_4 = 2,\ r_6 = 1, \\ r_1 = 9,\ r_3 = 5,\ r_5 = 1, \end{aligned}$$

de maneira que $S_P = 5+7+2+1 = 15$ e $S_I = 9+5+1 = 15$. Assim, $S_P - S_I = 0$, e como $11|0$, segue que $11|a$. Agora, para $b = 132349871$,

$$r_0 = 1,\ r_2 = 8,\ r_4 = 4,\ r_6 = 2,\ r_8 = 1,$$
$$r_1 = 7,\ r_3 = 9,\ r_5 = 3,\ r_7 = 3.$$

Logo, $S_P = 1+8+4+2+1 = 16$ e $S_I = 7+9+3+3 = 22$. Como $S_P - S_I = -5$ e $11 \nmid -5$, o número b não é divisível por 11.

4.3 Máximo Divisor Comum e Mínimo Múltiplo Comum

Nesta seção estudaremos dois conceitos fundamentais, que aparecem naturalmente em vários problemas de divisibilidade, assim como a relação existente entre eles.

O primeiro destes conceitos está relacionado com os inteiros positivos que dividem simultaneamente dois inteiros prefixados e é chamado *máximo divisor comum*. O segundo conceito está relacionado com os inteiros positivos que são simultaneamente múltiplos de dois inteiros prefixados e é denominado *mínimo múltiplo comum*.

4.3.1 Máximo Divisor Comum - MDC

Na escola secundária, quando do estudo do MDC, é comum considerar dois números naturais relativamente pequenos, determinar seus divisores positivos, identificar os divisores comuns e verificar o maior entre eles.

Numa linguagem mais técnica, o que se faz é o seguinte: tomemos a e b inteiros ambos não nulos e consideremos

$$D_a = \{n \in \mathbb{N} : n|a\} \text{ e } D_b = \{n \in \mathbb{N} : n|b\}.$$

É claro que $D_a \cap D_b \neq \emptyset$, pois $1|a$ e $1|b$. Além disso, de acordo com o Lema 4.7 (ii), $D_a \cap D_b$ é um conjunto finito e, por isso, possui maior elemento, chamado de *máximo divisor comum* (MDC) de a e b, o qual denotaremos por

$$(a,b).$$

Por exemplo, para $a = 18$ e $b = 24$, temos $D_a = \{1,2,3,6,9,18\}$ e $D_b = \{1,2,3,4,6,8,12,24\}$, de modo que $D_a \cap D_b = \{1,2,3,6\}$. Por isso, $(18,24) = 6$.

Por construção, temos claramente que $(a,b) = (b,a)$. Notemos ainda que se $a = b = 0$, então como qualquer número natural divide zero, segue que o conjunto D_a é infinito. É por isso que este caso não será considerado, mas acordamos que $(0,0) = 0$.

Definição 4.3 *Sejam $a,b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Diremos que $d \in \mathbb{N}$ é o* ***máximo divisor comum*** *de a e b quando as seguintes condições são satisfeitas:*

(i) $d|a$ *e* $d|b$.

(ii) Se $c|a$ *e* $c|b$*, então* $c|d$.

Em outras palavras, o máximo divisor comum de a e b é um número natural que divide e é divisível por todo divisor comum de a e b.

Em alguns casos particulares, é imediato calcular o *MDC*. Por exemplo, se a é um número inteiro não nulo, tem-se claramente que:

(i) $(0,a) = |a|$;

(ii) $(1,a) = 1$;

(iii) $(a,a) = |a|$.

Além disso, para todo $b \in \mathbb{Z}$,

$$a|b \Leftrightarrow (a,b) = |a|.$$

É imediato verificar que:

$$(a,b) = (-a,b) = (-a,-b) = (a,-b) = (b,a)$$

Por isso, vamos assumir que a e b são sempre positivos.

O teorema a seguir é fundamental para soluções de muitos problemas na *Teoria dos Números*, pois nos dá uma proveitosa identidade que relaciona os números a e b e seu *MDC*. Tal identidade é conhecida como identidade de **Bachet-Bézout**[3] para os inteiros a e b.

Teorema 4.12 ***(Bachet-Bézout)*** *Se* $d = (a,b)$*, então existem inteiros* $x_0, y_0 \in \mathbb{Z}$ *tais que*

$$d = ax_0 + by_0.$$

Demonstração: Consideremos o conjunto

$$W = \{ax + by : x,y \in \mathbb{Z} \ \ e \ \ ax + by > 0\}.$$

Note que W não é vazio, pois para $x = y = 1$,

$$a.1 + b.1 = a + b > 0 \Rightarrow a + b \in W.$$

[3] O matemático francês Claude-Gaspard Bachet $(1581 - 1638)$ foi quem primeiro provou este resultado, o qual foi posteriormente generalizado para polinômios pelo também matemático francês Étienne Bézout $(1730 - 1783)$.

Desse modo, pelo PBO, W possui menor elemento, digamos $\lambda = minW$. Vamos mostrar que $\lambda = (a,b)$. Como $\lambda \in W$, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$\lambda = ax_0 + by_0. \tag{4.4}$$

Usando o Algoritmo da Divisão com os elementos a e λ, temos

$$a = \lambda q + r, \ \ com \ \ 0 \leq r < \lambda. \tag{4.5}$$

Substituindo o valor de λ em (4.4) na igualdade de (4.5), segue que

$$\begin{aligned} r = a - \lambda q &= a - (ax_0 + by_0) \\ &= a - aqx_0 - bqy_0 \end{aligned}$$

Dái,

$$r = a(1 - qx_0) + b(-qy_0).$$

Isso nos mostra que $r = au + bv$, com $u = 1 - qx_0$ e $v = -qy_0$. Por conseguinte, $r = 0$, pois caso contrário, $r > 0$ e, assim, $r \in W$, o que contraria o fato de λ ser o mínimo de W, visto que $r < \lambda$. Portanto, $a = \lambda q$, ou seja, $\lambda | a$. Analogamente, prova-se que $\lambda | b$.

Sendo $d = (a,b)$, então $a = d\lambda_1$ e $b = d\lambda_2$. Logo, por (4.4),

$$\lambda = (d\lambda_1)x_0 + (d\lambda_2)y_0 = d(\lambda_1 x_0 + \lambda_2 y_0),$$

ou seja, $d|\lambda$, e como $\lambda | d$ pois $d = (a,b)$, segue que $d = \lambda$. Logo, $d = ax_0 + by_0$. ■

Pelo teorema anterior, se $d = (a,b)$, então podemos escrevê-lo na forma

$$d = ax_0 + by_0.$$

com $x_0, y_0 \in \mathbb{Z}$. Por isso, dizemos que d é uma *combinação linear*.[4] Além disso, tal combinação não é única.

Vamos denotar o conjunto de todos os múltiplos de um inteiro n (positivos, negativos ou zero) por $n\mathbb{Z}$.[5]

A prova do Teorema **Bachet-Bézout** nos mostra que $d = (a,b)$ é o menor inteiro positivo da forma $ax + by$, em que x e y são inteiros. Outro fato interessante é dado pelo seguinte:

Corolário 4.13 *Se $d = (a,b)$, então*

$$X = \{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z}.$$

[4] Uma combinação linear de a e b é toda expressão da forma $ax + by$, em que x e y são inteiros.

[5] Esta notação deve-se a Étienne Bézout.

Demonstração: Sendo $d = (a,b)$, então $a = du$ e $b = dv$, em que $u, v \in \mathbb{Z}$. Assim, dado $\alpha \in X$, segue que $\alpha = ax_0 + by_0$, com $x_0, y_0 \in \mathbb{Z}$, de modo que $\alpha = d(ux_0 + vy_0)$, ou seja, $\alpha \in d\mathbb{Z}$ e, assim $X \subset d\mathbb{Z}$. Para outra inclusão, sabemos pelo Teorema (4.12) que $d = ax_1 + by_1$, com $x_1, y_1 \in \mathbb{Z}$. Desse modo, para qualquer $dm \in d\mathbb{Z}$,

$$dm = a(mx_1) + b(my_1) \in X.$$

Logo, $d\mathbb{Z} \subset X$, o que mostra que $d\mathbb{Z} = X$. ■

4.3.2 Algoritmo de Euclides

O Lema a seguir, chamado por **Lema de Euclides**, será fundamental para estabelecer o Algoritmo de Euclides, que permitirá, com muita eficácia, calcular o Máximo Divisor Comum de dois números naturais quaisquer.

Lema 4.14 ***(Lema de Euclides)*** *Sejam $a, b, n \in \mathbb{Z}$. Então*

$$(a,b) = (a, b - na).$$

Demonstração: Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto, $c|d$. Isso prova que $d = (a,b)$. ■

O lema anterior é efetivo para calcular o MDC, conforme veremos nos exemplos a seguir:
Exemplo 4.3 Calcular $(48, 76)$ utilizando o Lema de Euclides.

Solução: Pelo Lema de Euclides, temos

$$\begin{aligned}
(48,76) = (48,76-1(48)) = (48,28) &= (28,48-1(28)) \\
&= (28,20) \\
&= (20,28-1(20)) \\
&= (20,8) \\
&= (8,20-2(8)) \\
&= (8,4) \\
&= (4,8-2(4)) \\
&= (4,0).
\end{aligned}$$

Portanto, o $(48,76) = (4,0) = 4$. ▲

Exemplo 4.4 Seja $n \in \mathbb{N}$. Mostre que $(n+1, n^2+n+1) = 1$.

Solução: Pelo Lema de Euclides, temos

$$\begin{aligned}(n+1, n^2+n+1) &= (n+1, n^2+n+1-(n+1)) \\ &= (n+1, n^2) \\ &= (n+1, n^2-n(n+1)) \\ &= (n+1, -n) \\ &= (n+1, -n+n+1) \\ &= (n+1, 1) \\ &= 1\end{aligned}$$

▲

Definição 4.4 *Dois inteiros a e b são ditos* ***primos entre si*** *ou* ***relativamente primos*** *quando* $(a,b) = 1$.

Como consequência imediata do Teorema de **Bachet-Bézout**, temos:

Corolário 4.15 *Os inteiros a e b são relativamente primos se, e somente se, existem* $x, y \in \mathbb{Z}$ *tais que* $ax + by = 1$.

Demonstração: ($\Rightarrow$) Se $(a,b) = 1$, então o Teorema de **Bachet-Bézout** assegura a existência de inteiros x e y tais que $ax + by = 1$.
($\Leftarrow$) Agora, suponha que $ax + by = 1$ para $x, y \in \mathbb{Z}$, e seja, $d = (a,b)$. Como $d|a$ e $d|b$, então $d|ax + by = 1$. Como $d > 0$, temos que $d = 1$, ou seja, a e b são relativamente primos. ■

Teorema 4.16 ***(Lema de Gauss)*** *Sejam* $a, b, c \in \mathbb{Z}$. *Se* $a|bc$ *e* $(a,b) = 1$, *então* $a|c$.

Demonstração: Por hipótese, $bc = ak$, com $k \in \mathbb{Z}$. Além disso, pelo Corolário 4.15, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Logo, multiplicando ambos os lados desta igualdade por c, obtemos

$$\begin{aligned}ax + by = 1 \Rightarrow c = cax + cby &= cax + aky \\ &= a(cx + ky).\end{aligned}$$

Desse modo, $a|c$. ■

Corolário 4.17 *Sejam $a,b \in \mathbb{Z}$ tais que $(a,b) = 1$. Se $a|c$ e $b|c$, então $ab|c$.*

Demonstração: Como $(a,b) = 1$, então pela identidade de Bachet-Bézout, existem $x,y \in \mathbb{Z}$ tais que

$$ax + by = 1 \tag{4.6}$$

Por outro lado, existem $q_1, q_2 \in \mathbb{Z}$ satisfazendo $c = aq_1 = bq_2$, de modo que

$$cb = abq_1 \;\; e \;\; ca = abq_2.$$

Logo, multiplicando os lados da igualdade em (2.3) por c, obtemos

$$\begin{aligned} c = cax + cby &= abq_2x + abq_1y \\ &= ab(q_2x + q_1y), \end{aligned}$$

isto é, $ab|c$. ■

Corolário 4.18 *Dados $a,b,c \in \mathbb{Z}$, com b e c não nulos, temos que*

$$b|a \;\; e \;\; c|a \Leftrightarrow \frac{bc}{(b,c)}|a.$$

Demonstração: Como $b|a$ e $c|a$, então existem $m,n \in \mathbb{Z}$, tais que $mb = a$ e $nc = a$. assim $mb = nc$. Multiplicando ambos os lados da última igualdade por $\frac{1}{(b,c)}$, temos

$$n\frac{b}{(b,c)} = m\frac{c}{(b,c)}.$$

Como $(\frac{b}{(b,c)}, \frac{c}{(b,c)}) = 1$, segue-se que $\frac{b}{(b,c)}|m$, o que implica que $\frac{b}{(b,c)}c|mc$. Como, $mc = a$ então, $\frac{bc}{(b,c)}|a$.

Reciprocamente, se $\frac{bc}{(b,c)}|a$ então existe $m \in \mathbb{Z}$ tal que

$$\frac{bc}{(b,c)}m = a \Rightarrow bcm = a(b,c)$$

pelo **Lema de Gauss**, segue que $b|a \;\; e \;\; c|a$. ■

A noção de MDC pode ser generalizada como a seguir.

Um número natural d será dito MDC de dados números inteiros $a_1, ..., a_n$ não todos nulos, se possuir as seguintes condições:

(i) d é um divisor comum de $a_1, ..., a_n$.

(ii) Se c é um divisor comum de $a_1, ..., a_n$, então $c|d$.

O MDC, é certamente único e será representado por

$$(a_1, ..., a_n).$$

A proposição a seguir nos fornece um método indutivo para o cálculo de MDC de n inteiros, reduzindo-o à aplicação do *Algoritmo de Euclides* a $n-1$ pares de inteiros.

Proposição 4.19 *Dados números inteiros $a_1, ..., a_n$, não todos nulos, existe o seu MDC e*

$$(a_1, ..., a_n) = (a_1, ..., (a_{n-1}, a_n))$$

Demonstração: Vamos provar a proposição por indução sobre $n \geq 2$. Para $n = 2$, nada temos a provar.

Suponha que o resultado seja válido para n. Para provar que o resultado é válido para $n+1$, basta mostrar que se d é o MDC de $a_1, ..., (a_n, a_{n+1})$, então d é o MDC de $a_1, ..., a_n, a_{n+1}$, pois isso provará também a existência.

Seja d o MDC de $a_1, ..., (a_n, a_{n+1})$. Logo, $d|a_1, ..., d|a_{n-1}$ e $d|(a_n, a_{n+1})$. Portanto, $d|a_1, ..., d|a_{n-1}, d|a_n$ e $d|a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, ..., a_n, a_{n+1}$; logo c é divisor comum de $a_1, ..., a_{n-1}$ e (a_n, a_{n+1}); e portanto. $c|d$. ■

4.3.3 Mínimo Múltiplo Comum - MMC

O conceito de Mínimo Múltiplo Comum (MMC) é um paralelo importante do conceito de MDC.

Definição 4.5 *Sejam a e b inteiros não nulos. O número $m \in \mathbb{N}$ é o **mínimo múltiplo comum** de a e b quando as seguintes condições são satisfeitas:*

(i) $a|m$ e $b|m$.

(ii) Se $a|c$ e $b|c$, então $m|c$.

O mínimo múltiplo comum de a e b, se existe, é denotado por $[a, b]$.

Caso exista $[a, b]$, é fácil mostrar que

$$[-a, b] = [a, -b] = [-a, -b] = [a, b] = [b, a].$$

Assim, para efeito de cálculo do MMC de dois números, podemos sempre supô-los não negativos.

É também fácil verificar que $[a,b] = 0$ se, e somente se, $a = 0$ ou $b = 0$. De fato, se $[a,b] = 0$, então 0 divide ab, que é múltiplo de a e b, logo $ab = 0$ e, portanto, $a = 0$ ou $b = 0$. Reciprocamente, se $a = 0$ ou $b = 0$, então 0 é o único múltiplo comum de a e b, logo $[a,b] = 0$.

Proposição 4.20 *Dados dois números naturais a e b, com $d = (a,b)$ e $m = [a,b]$, temos que*

$$[a,b](a,b) = ab \Rightarrow m = \frac{ab}{d}$$

Demonstração: Consideremos $m_1 = \frac{ab}{d}$ e provemos que $m_1 = m$. Como, $d|a$ e $d|b$, então $a = d\lambda_1$ e $b = d\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{N}$. Assim,

$$m_1 = \frac{ab}{d} = \frac{\lambda_1 db}{d} = \lambda_1 b \Rightarrow b|m_1.$$

Da mesma forma, prova-se que $a|m_1$. Tomemos agora m_2 outro múltiplo comum de a e b, isto é, $m_2 = a\alpha_1$ e $m_2 = a\alpha_2$, com $\alpha_1, \alpha_2 \in \mathbb{N}$. Pela identidade de Bachet-Bézout, existem inteiros x e y tais que $d = ax + by$. Logo,

$$\begin{aligned} \frac{m_2}{m_1} = \frac{m_2 d}{m_1 d} &= \frac{axm_2 + bym_2}{ab} \\ &= \frac{ab\alpha_2 x + ab\alpha_1 y}{ab} \\ &= \alpha_2 x + \alpha_1 y \in \mathbb{Z}, \end{aligned}$$

ou seja, $m_1|m_2$. Portanto, isso mostra que $m_1 = m = \frac{ab}{d}$. ■

De acordo com a proposição anterior, $[a,b] \leq ab$. Além disso, o cálculo de $d = (a,b)$, o que é feito de forma prática através do Algoritmo de Euclides, implica diretamente no cálculo de $m = [a,b]$. Para tanto, basta dividir o produto ab por d.

Uma consequência imediata é a seguinte:

Corolário 4.21 *Dados $a,b \in \mathbb{N}$, temos que o $[a,b] = ab$ se, e somente se, a e b são primos entre si.*

Podemos estender a noção de MMC para vários números, como faremos a seguir.

Considerando n números naturais $a_1, a_2, ..., a_n$, podemos mostrar que estes números possuem mínimo múltiplo comum, denotado por $[a_1, a_2, ..., a_n]$, tal que

$$[a_1, a_2, ..., a_n] = [m_1, a_3, ..., a_n],$$

sendo $m_1 = [a_1, a_2]$, ou seja, calculamos o $[a_1, a_2, ..., a_n]$ em $n-1$ passos através da sequência de números

$$m_1 = [a_1, a_2], \;\; m_2 = [(m_1, a_3), ..., m_{n-1}] = [m_{n-2}, a_n]$$

e m_{n-1} é o mínimo múltiplo comum de $a_1, a_2, ..., a_n$.

Proposição 4.22 *Sejam $a_1, a_2, ..., a_n$ e k números naturais. Então,*

$$[ka_1, ka_2, ..., ka_n] = k.[a_1, a_2, ..., a_n].$$

Demonstração: Consideremos

$$m_1 = [ka_1, ka_2, ..., ka_n] \;\; e \;\; m = [a_1, a_2, ..., a_n].$$

Como $m = a_i\lambda_i$ para $i = 1, ..., n$, segue que $km = a_i(k\lambda_i)$, isto é, km é múltiplo de $ka_1, ka_2, ..., ka_n$, de maneira que $km \geq m_1$. Por outro lado, como m_1 é múltiplo comum de $ka_1, ka_2, ..., ka_n$, então $m_1 = ka_i\alpha_i$, com $i = 1, ..., n$, e por isso, $\frac{m_1}{k}$ é múltiplo de $a_1, a_2, ..., a_n$. Desse modo, $\frac{m_1}{k} > m$, ou seja, $m_1 \geq km$. Isso mostra que $m_1 = km$. ■

4.4 Números Primos

Sabemos que toda matéria é formada por pequenas partículas: os átomos. Os gregos antigos foram os primeiros a saber que a matéria é formada por tais partículas e o filósofo grego Demócrito (que viveu entre 546 e 460 a.C.) foi quem denominou essas partículas de átomos (do grego: a= não; tomo= divisão), pois acreditava que, de fato, elas eram indivisíveis. Hoje se sabe que os átomos podem ser divididos em partículas menores, mas a ideia de que a matéria existe em *unidades mínimas* segue vigente.

Na Aritmética, essa ideia de *unidades mínimas* também existe e veio da Grécia antiga. Só que o papel dos átomos, neste caso, é exercido pelos chamados *números primos*. Os pitagóricos (de 500 a 300 a.C., mais ou menos) foram os primeiros a se interessarem pelas propriedades *místicas* desses números.

Mas, diferentemente dos átomos de verdade, os *números primos* continuam e vão continuar funcionando como blocos numéricos fundamentais, responsáveis por gerar todos os números inteiros diferentes de 0 e de ± 1. Esta propriedade é conhecida como *Teorema Fundamental da Aritmética (TFA)*.

4.4.1 Teorema Fundamental da Aritmética - TFA

Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de *número primo*.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

(i) Se $p|q$, então $p = q$.

(ii) Se $p \nmid a$, então $(p,a) = 1$.

Demonstração:

(i) Como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

(ii) Se $(p,a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

■

Definição 4.6 *Um número maior do que* 1 *e que não é primo será dito composto. Portanto, se um número natural* $n > 1$ *for composto, existirá um divisor natural* n_1 *de* n *tal que* $1 < n_1 < n$*. Logo, existirá um número natural* n_2 *tal que*

$$n = n_1 n_2, \ \ com \ \ 1 < n_1 < n \ \ e \ \ 1 < n_2 < n$$

A seguir, estabelecemos um resultado fundamental de Euclides, chamado *Lema de Euclides*[6]

Proposição 4.23 *Sejam* $a, b \in \mathbb{Z}$ *e* p *um número primo. Se* $p|ab$*, então* $p|a$ *ou* $p|b$*.*

Demonstração: Como p é primo, então $(a,p) = 1$ ou $(a,p) = p$. Se $p \nmid a$, então $(a,p) = 1$. Portanto, de acordo com o Lema de Gauss (Teorema 4.16), temos que $p|b$. ■

O resultado anterior pode ser estendido para um produto de n inteiros, vejamos:

Corolário 4.24 *Se* p *é primo e* $p|a_1 a_2 ... a_n$*, então* $p|a_i$ *para algum* $i = 1, ..., n$*.*

Demonstração: Provemos por indução sobre n.
Para $n = 1$ o resultado é imediato. Suponhamos, por hipótese de indução, que o resultado seja válido para $n \geq 1$. Logo, para $a_1, a_2, ..., a_n, a_{n+1} \in \mathbb{Z}$, temos

$$\begin{aligned} p|a_1 a_2 ... a_n a_{n+1} &\Rightarrow p|(a_1 a_2 ... a_n)a_{n+1} \\ &\Rightarrow p|(a_1 a_2 ... a_n) \ \ ou \ \ p|a_{n+1} \end{aligned}$$

Se $p|a_{n+1}$, o resultado segue. Se $p|(a_1 a_2 ... a_n)$, então, por hipótese de indução, $p|a_i$ para algum $i = 1, ..., n$. ■

[6] *Os Elementos,* Proposição 30, Livro VII.

Corolário 4.25 *Se $p, q_1, q_2, ..., q_n$ são números primos e $p|q_1q_2...q_n$, então $p = q_i$ para algum $i = 1, ..., n$.*

Demonstração: Se $p|q_1q_2...q_n$, segue do corolário anterior que $p|q_i$ para algum $i = 1, ..., n$. Como q_i é primo, seus únicos divisores positivos são 1 e q_i. Logo, $p = q_i$, pois $p > 1$. ■

Teorema 4.26 ***(Teorema Fundamental da Aritmética - TFA)*** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Para prova usaremos Princípio de Indução. Se $n = 2$, o resultado é claramente verificado.

Suponhamos o resultado válido para todo númeno natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$. Portanto, $n = p_1...p_rq_1...q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1...p_r = q_1...q_s$, onde os p_i e os q_j são números primos. Como $p_1|q_1...q_s$, pelo corolário anterior, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1...q_s$, podemos supor que seja q_1. Portanto,

$$p_2...p_r = q_2...q_s$$

Como $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

Teorema 4.27 *Dado um número inteiro $n \neq 0, 1, -1$, existem primos $p_1 < ... < p_r$ e $\alpha_1 < ... < \alpha_r \in \mathbb{N}$, univocamente determinados, tais que*

$$n = \pm p_1^{\alpha_1}...p_r^{\alpha_r}.$$

Quando estivermos lidando com a decomposição em fatores primos de dois ou mais números naturais, usaremos o recurso de acrescentar fatores da forma $p^0(= 1)$, onde p é um número primo qualquer. Assim, dados $n, m \in \mathbb{N}$ com $n > 1$ e $m > 1$ quaisquer, podemos escrever

$$n = p_1^{\alpha_1}...p_r^{\alpha_r} \ \ e \ \ m = p_1^{\beta_1}...p_r^{\beta_r},$$

usando o mesmo conjunto de primos $p_1, ..., p_r$, desde que permitamos que os expoentes $\alpha_1 < ... < \alpha_r$, $\beta_1 < ... < \beta_r$ variem em $\mathbb{N} \cup \{0\}$ e não apenas em $\mathbb{N}$.

Observe que um número natural $n > 1$, escrito na **forma canônica** $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, como no teorema acima, é um *quadrado perfeito* se, e somente se, cada expoente α_i é par.

Teorema 4.28 *Se $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ é a fatoração canônica de $n > 1$, então um inteiro d é um divisor positivo de a se, e somente se,*

$$d = p_1^{\beta_1}...p_r^{\beta_r},$$

em que $0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, ..., r$.

Demonstração: Se $d = p_1^{\beta_1}...p_r^{\beta_r}$, com $0 \leq \beta_i \leq \alpha_i$, então $\alpha_i = \beta_i + k_i$ para cada $i = 1, ..., r$. Desse modo,

$$\begin{aligned} n = p_1^{\alpha_1}...p_r^{\alpha_r} &= p_1^{(\beta_1+k_1)}...p_r^{(\beta_r+k_r)} \\ &= (p_1^{\beta_1}...p_r^{\beta r})(p_1^{k_1}...p_r^{k_r}) \\ &= d.p_1^{k_1}...p_r^{k_r} \end{aligned}$$

isto é, $d|n$.

Reciprocamente, suponhamos que $d|n$, ou seja, $n = dc$ para algum c. De acordo com o TFA, tomemos

$$c = p_1^{k_1}...p_r^{k_r} \;\; e \;\; d = p_1^{\beta_1}...p_r^{\beta r},$$

em que $0 \leq \beta_i$ e $0 \leq k_i$ para $i = 1, ..., r$. Logo,

$$p_1^{\alpha_1}...p_r^{\alpha_r} = (p_1^{\beta_1}...p_r^{\beta r})(p_1^{k_1}...p_r^{k_r}) = p_1^{(\beta_1+k_1)}...p_r^{(\beta_r+k_r)}.$$

Pelo TFA, devemos necessariamente ter

$$\alpha_i = \beta_i + k_i \;\; para \;\; cada \;\; i = 1, ..., r.$$

Como $0 \leq k_i$, então $\beta_i \leq \alpha_i$ para cada $i = 1, ..., r$. ■

Denotando por $d(n)$ o número de divisores positivos do número natural n, segue, imediatamente, que se $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, onde $p_1, ..., p_r$ são números primos e $\alpha_1, ..., \alpha_r \in \mathbb{N}$, então

$$d(n) = (\alpha_1 + 1)...(\alpha_r + 1).$$

Teorema 4.29 *Sejam $a = p_1^{r_1}...p_n^{r_n}$ e $b = p_1^{s_1}...p_n^{s_n}$, sendo $p_1, ..., p_n$ primos distintos e $r_i, s_i \in \mathbb{N} \cup \{0\}$. Então,*

$$(a, b) = p_1^{\alpha_1}...p_n^{\alpha_n}, \;\; com \;\; \alpha_i = min\{r_i, s_i\}, \;\; 1 \leq i \leq n$$

e

$$[a, b] = p_1^{\beta_1}...p_n^{\beta n}, \;\; com \;\; \beta = max\{r_i, s_i\}, \;\; 1 \leq i \leq n,$$

em que $min\{r_i, s_i\}$ e $max\{r_i, s_i\}$ indicam o mínimo e máximo entre r_i e s_i, respectivamente.

Demonstração: Pelo teorema anterior, $d = p_1^{\alpha_1}...p_n^{\alpha_n}$, com $\alpha_i = min\{r_i, s_i\}$, é um divisor comum de a e b. Além disso, se d_1 é outro divisor de a e b, então

$$d_1 = p_1^{t_1}...p_n^{tn},$$

com $t_i \leq r_i$ e $t_i \leq s_i$ para cada $i = 1, ..., n$. Logo, $t_i \leq min\{r_i, s_i\} = \alpha_i$, ou seja, d_1 divide d, implicando que $d = (a, b)$. De modo análogo, prova-se a asserção sobre o MMC. ■

Na Teoria dos Números, é muito comum questionar se um dado número natural é primo ou não e, além disso, como decidir a respeito.

Dentre os métodos clássicos usados para responder a esta pergunta, destaca-se o Teste da Primalidade, que nos conduz a um algoritmo, chamado **Crivo de Erastóstenes**[7], que nos auxilia a determinar todos os números primos menores ou iguais a um dado número natural n.

Teorema 4.30 *Se $n > 1$ for composto, então n possui, necessariamente, um divisor primo p tal que $p \leq \sqrt{n}$. Ou seja, se n não possui divisores diferentes de 1, menores ou iguais a $\sqrt{n}$, então n é primo.*

Demonstração: Sendo n um número composto, então

$$n = a.b, \ \ com \ \ 1 < a, b < n.$$

Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = a.b > \sqrt{n}.\sqrt{n} = n,$$

o que é impossível. Logo, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Suponhamos que $a \leq \sqrt{n}$. Como $a > 1$, então existe um primo p, com $p|a$. Desde que $a|n$, temos que $p|n$ e $p \leq a \leq \sqrt{n}$. ■

Exemplo 4.5 Para o número $n = 151$, temos que $[\sqrt{n}] = 12$ e os primos menores que 12 são 2, 3, 5, 7 e 11. Como nenhum destes primos divide n, concluímos que n é primo. Já $n = 217$ é composto, pois $[\sqrt{n}] = 14$ e 7 divide 217. ▲

4.4.2 Decomposição do Fatorial em Primos

Nesta Seção, iremos mostrar como a fatoração em números primos de $n!$, onde n é um número natural arbitrário.

[7] A palavra crivo significa peneira. O método consiste em separar os números naturais em um intervalo $[2, n]$, jogando fora os números que não são primos

Se a e b são números naturais, denotaremos pelo símbolo $\left[\frac{a}{b}\right]$ o quociente da divisão euclidiana de a por b, que é o maior inteiro menor ou igual do que o número racional $\frac{a}{b}$. Ou seja, $\left[\frac{a}{b}\right]$ representa a parte inteira da divisão de a por b.

Proposição 4.31 *Sejam $a, b, c \in \mathbb{N}$. Temos que*

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right].$$

Demonstração: Consideremos

$$q_1 = \left[\frac{a}{b}\right] \text{ e } q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right].$$

Assim,

$$a = bq_1 + r_1, \text{ com } 0 \leq r_1 < b$$

e

$$q_1 = \left[\frac{a}{b}\right] = cq_2 + r_2 \text{ com } 0 \leq r_2 < c.$$

Logo, substituindo $q_1 = cq_2 + r_2$ em $a = bq_1 + r_1$, obtemos

$$a = b(cq_2 + r_2) + r_1 = bcq_2 + (br_2 + r_1).$$

O que devemos mostrar é que $br_2 + r_1 \leq bc - 1$. De fato, como $0 \leq r_1 \leq b - 1$ e $0 \leq r_2 \leq c - 1$, segue que

$$br_2 + r_1 \leq b(c-1) + b - 1 = bc - 1.$$

Por isso, q_2 é o quociente da divisão de a por bc, isto é, $q_2 = \left[\frac{a}{bc}\right]$. ■

O que acabamos de provar enuncia-se com palavras como: *o quociente da divisão por c do quociente da divisão de a por b é igual ao quociente da divisão de a por b vezes c.*

Definição 4.7 *Seja p um número primo. Dado um número natural m, definimos $E_p(m)$ como o expoente da maior potência de p que divide m, ou seja, o expoente da potência de p que aparece na fatoração de m em fatores primos.*

Em particular, $E_p(n!)$ representa a potência de p que aparece na fatoração de $n!$ em fatores primos. O Resultado que segue deve-se a Adrien-Marie Legendre[8] que nos mostra como calcular $E_p(n!)$.

[8]Foi um matemático francês que teve importantes contribuições para a estatística, teoria dos números, álgebra abstrata e análise matemática. Algumas fontes afirmam que Legendre nasceu em Paris, enquanto outras afirmam ter sido em Toulouse, mas o que se pode afirmar com certeza é que ele nasceu em 18 de setembro de 1752.

Teorema 4.32 *Sejam p primo e $n \geq 1$ um número natural. Então,*

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Demonstração: Note, inicialmente que a soma acima é finita, pois existe $k \in \mathbb{N}$ tal que $p^i > n$ para todo $i \geq k$, ou seja,

$$\left[\frac{n}{p^i}\right] = 0$$

sempre que $i \geq k$. Mostremos o resultado usando a segunda forma de indução finita sobre n. Para $n = 1$ o resultado segue, pois $E_p(1!) = 0$. Suponhamos, por hipótese de indução, que o resultado seja válido para todo número natural m tal que $1 \leq m < n$. Desde que os múltiplos de p entre 1 e n são

$$p, 2p, \ldots, \left[\frac{n}{p}\right]p,$$

temos

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p\left(\left[\frac{n}{p}\right]!\right).$$

Como $\frac{n}{p} < n$, segue por hipótese de indução que

$$E_p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p^2}\right] + \cdots$$

Portanto, pela Proposição 4.31, obtemos

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

■

No que segue, ao dizermos que *r é o número de zeros de a*, queremos dizer que *a termina com r zeros consecutivos*. Por exemplo, para $a = 23012000$, temos $r = 3$, e para $a = 36082$, $r = 0$ (a não termine em zero).

Teorema 4.33 *O número de zeros de n! é igual a*

$$min\{E_2(n!), E_5(n!)\}.$$

Demonstração: Consideremos $E_2(n!) = \alpha$ e $E_5(n!) = \beta$. O número de zeros de $n!$ é exatamente igual a maior potência de $10 = 2.5$ que divide $n!$. Como essa potência é igual a

$$10^{min\{\alpha,\beta\}},$$

então o número de zeros de $n!$ é igual ao $min\{E_2(n!), E_5(n!)\}$. ■

Como consequência imediata do teorema anterior, temos:

Corolário 4.34 *Se $n \geq 5$, então o número de zeros de $n!$ é igual a $E_5(n!)$. Para $n < 5$, $n!$ não tem zero.*

Exemplo 4.6 Determinar com quantos zeros termina o número 100!.

Solução: Pelo corolário anterior, o número de zeros de 100! é igual a $E_5(100!)$. Como

$$E_5(100!) = \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] = 20 + 4 = 24$$

▲

Exemplo 4.7 Vamos determinar a decomposição de 30! em fatores primos e descobrir com quantos zeros termina a representação decimal desse número.

Solução: Para resolver o problema, deveremos achar $E_p(30!)$ para todo primo $p \leq 30$. Estes primos são $p = 2, 3, 5, 7, 11, 13, 17, 19, 23$ e 29.

Sendo

$$\begin{aligned}
E_2(30!) &= \left[\frac{30}{2}\right]+\left[\frac{30}{2^2}\right]+\left[\frac{30}{2^3}\right]+\left[\frac{30}{2^4}\right]=15+7+3+1=26,\\
E_3(30!) &= \left[\frac{30}{3}\right]+\left[\frac{30}{3^2}\right]+\left[\frac{30}{3^3}\right]=10+3+1=14,\\
E_5(30!) &= \left[\frac{30}{5}\right]+\left[\frac{30}{5^2}\right]=6+1=7,\\
E_7(30!) &= \left[\frac{30}{7}\right]=4,\\
E_{11}(30!) &= \left[\frac{30}{11}\right]=2,\\
E_{13}(30!) &= \left[\frac{30}{13}\right]=2,\\
E_{17}(30!) &= \left[\frac{30}{17}\right]=1,\\
E_{19}(30!) &= \left[\frac{30}{19}\right]=1,\\
E_{23}(30!) &= \left[\frac{30}{23}\right]=1,\\
E_{29}(30!) &= \left[\frac{30}{29}\right]=1.
\end{aligned}$$

Portanto, $30! = 2^{26}.3^{14}.5^7.7^4.11^2.13^2.17.19.23.29$, e como $E_5(30!) = 7$, segue que $30!$ termina com sete zeros. ▲

Capítulo 5

Congruência

5.1 Congruência

Grande parte dos resultados deste capítulo foi introduzida por Gauss $(1777-1855)$ em um trabalho publicado em 1801 denominado de *Disquisitiones Arithmeticae* quando tinha apenas 24 anos. Várias ideias de grande importância, que serviram de base para o desenvolvimento da Teoria dos Números aparecem neste trabalho. Até mesmo a notação, lá introduzida, é a que utilizamos hoje.

Definição 5.1 *Sejam m um número natural e a e b inteiros quaisquer. Dizemos que a é* ***congruente*** *a b **módulo** m, e escrevemos*

$$a \equiv b (mod\ m),$$

quando m divide $b-a$. Se $m \nmid (b-a)$, dizemos que a é incongruente a b módulo m e escrevemos

$$a \not\equiv b (mod\ m).$$

Proposição 5.1 *Se a e b são inteiros, temos que $a \equiv b (mod\ m)$ se, e somente se, existe um inteiro k tal que $a = b + km$.*

Demonstração: Se $a \equiv b (mod\ m)$, então $m|(b-a)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$.

Reciprocamente, suponha a existência de um inteiro k satisfazendo a igualdade $a = b + km$, ou seja, $km = a - b$, o que implica que $m|(b-a)$, isto é, $a \equiv b (mod\ m)$. ■

Proposição 5.2 *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras.*

(i) $a \equiv a (mod\ m)$.

(ii) Se $a \equiv b (mod\ m)$, *então* $b \equiv a (mod\ m)$.

(iii) Se $a \equiv b(mod\ m)$ *e* $b \equiv d(mod\ m)$*, então* $a \equiv d(mod\ m)$.

Demonstração:

(i) Como $m|0$, então $m|(a-a)$, o que implica $a \equiv a(mod\ m)$.

(ii) Se $a \equiv b(mod\ m)$, então $a - b = mk.$ com $k \in \mathbb{Z}$. Logo, $b - a = m(-k)$ e $-k \in \mathbb{Z}$, isto é, $b \equiv a(mod\ m)$.

(iii) Assumindo que $a \equiv b(mod\ m)$ e $b \equiv d(mod\ m)$, existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$a - b = mk_1 \text{ e } b - c = mk_2.$$

Somando membro a membro estas duas igualdades, obtemos $a - d = mk_3$, com $k_3 = k_1 + k_2 \in \mathbb{Z}$, ou seja, $a \equiv d(mod\ m)$.

■

Esta proposição nos diz que a relação de congruência, definida no conjunto dos inteiros é uma relação de equivalência, pois acabamos de provar que ela é *reflexiva*, *simétrica* e *transitiva*.

Teorema 5.3 *Se* a, b, c *e* m *são inteiros tais que* $a \equiv b(mod\ m)$*, então*

(i) $a + c \equiv b + c(mod\ m)$.

(ii) $a - c \equiv b - c(mod\ m)$.

(iii) $ac \equiv bc(mod\ m)$.

Demonstração:

(i) Como $a \equiv b(mod\ m)$, então existe $k \in \mathbb{Z}$ tal que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c(mod\ m)$.

(ii) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$, $k \in \mathbb{Z}$, temos que $a - c \equiv b - c(mod\ m)$.

(iii) Como $a - b = km$, $k \in \mathbb{Z}$ então $ac - bc = ckm$ o que implica $m|(ac - bc)$ e, portanto, $ac \equiv bc(mod\ m)$.

■

Teorema 5.4 *Se* a, b, c, d *e* m *são inteiros tais que* $a \equiv b(mod\ m)$*, e* $c \equiv d(mod\ m)$*, então*

(i) $a + c \equiv b + d(mod\ m)$.

(ii) $a - c \equiv b - d (mod\ m)$.

(iii) $ac \equiv bd (mod\ m)$

Demonstração:

(i) De $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$ temos $a - b = km$ e $c - d = k_1 m$, $k, k_1 \in \mathbb{Z}$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica $a + c \equiv b + d (mod\ m)$.

(ii) Basta substituir membro a membro $a - b = km$ e $c - d = k_1 m$ obtendo $(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1)m$, $k, k_1 \in \mathbb{Z}$, o que implica $a - c \equiv b - d (mod\ m)$.

(iii) Multiplicando ambos os lados de $a - c = km$ por c e ambos os lados de $c - d = k_1 m$ por b, com $k, k_1 \in \mathbb{Z}$, obtemos $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $ac - bc + bc - bd = ac - bd = (ck + bk_1)m$ o que implica $ac \equiv bd (mod\ m)$.

■

Definição 5.2 *Um conjunto de inteiros* $\{a_1, \ldots, a_r\}$ *é um* ***sistema completo de resíduos módulo*** *m quando:*

(i) $a_i \not\equiv a_j (mod\ m)$ *para* $i \neq j$.

(ii) Para todo inteiro b, existe a_i *tal que* $b \equiv a_i (mod\ m)$.

Note que, todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos número $0, 1, \ldots, m - 1$. Além disso, qualquer par de números distintos deste conjunto são incongruentes módulo m.

Assim, para achar o resto da divisão de um número a por m, basta achar o número natural r dentre os números $0, 1, \ldots, m - 1$ que seja congruente a a módulo m. Portanto, um sistema completo de resíduos módulo m possui m elementos.

É claro que se $a_1, \ldots, a_m$ são m números inteiros, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números $0, 1, \ldots, m - 1$ em alguma ordem. Em particular, um conjunto formado por m inteiros consecutivos é um sistema completo de resíduos módulo m.

Seja R um sistema completo de resíduos módulo m. Então, a divisão euclidiana por m pode ser generalizada como segue:

Para todo $a \in \mathbb{Z}$ existem inteiros q e r univocamente determinados tais que

$$a = mq + r, \text{ com } r \in R.$$

Nessa divisão dizemos tratar-se da **divisão com resto** em $R = \{0, 1, ..., m-1\}$.

Corolário 5.5 *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b(mod\ m)$, então tem-se que $a^n \equiv b^n(mod\ m)$.*

Demonstração: A demonstração faz-se por indução sobre n. Vejamos

(i) Para $n = 1$, a sentença é verdadeira, pois

$$a^1 \equiv b^1(mod\ m) \Rightarrow a \equiv b(mod\ m)$$

(ii) Suponha a sentença verdadeira para algum $n \in \mathbb{N}$ e mostremos que vale para $n+1$. Logo,

$$a \equiv b(mod\ m) \Rightarrow a^n.a \equiv b^n.b(mod\ m) \Rightarrow a^{n+1} \equiv b^{n+1}(mod\ m).$$

Logo, a sentença vale para $n+1$. Portanto, $a^n \equiv b^n(mod\ m)$ para todo $n \in \mathbb{N}$. ■

Proposição 5.6 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que*

$$a + c \equiv b + c(mod\ m) \Leftrightarrow a \equiv b(mod\ m).$$

Demonstração: Se $a \equiv b(mod\ m)$, segue imediatamente do Teorema 5.4(i) que $a + c \equiv b + c(mod\ m)$, pois $c \equiv c(mod\ m)$.

Reciprocamente, se $a + c \equiv b + c(mod\ m)$, então $m|b + c - (a + c)$, o que implica que $m|b - a$ e consequentemente, $a \equiv b(mod\ m)$. ■

A proposição acima nos diz que, para as congruências, vale o cancelamento com relação à adição. Quando é multiplicação isto em geral nem sempre é verificado, conforme a Corolário 5.8.

Teorema 5.7 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que*

$$ac \equiv bc(mod\ m) \Leftrightarrow a \equiv b(mod\ \frac{m}{d}),$$

onde $d = (c, m)$.

Demonstração: Se $ac \equiv bc(mod\ m)$, então

$$ac - bc = c(a - b) = km, \ \ com\ \ k \in \mathbb{Z}. \tag{5.1}$$

Sendo $d = (c, m)$, então $m = dr$ e $c = ds$, em que r e s são primos entre si, pois $(r, s) = (\frac{m}{d}, \frac{c}{d}) = 1$. Substituindo os valores de m e c em (5.1), obtemos

$$ds(a - b) = kdr \Rightarrow s(a - b) = kr \Rightarrow r|s(a - b),$$

de modo que $r|(a-b)$, pois $(r,s)=1$. Logo, $a \equiv b(mod\ r)$, ou melhor, $a \equiv b(mod\ \frac{m}{d})$. Reciprocamente, sejam, $c = d\lambda_1$ e $m = d\lambda_2$. Como $a \equiv b(mod\ \frac{m}{d})$, isto é, $a \equiv b(mod\ \lambda_2)$, então $a - b = k\lambda_2$, com $k \in \mathbb{Z}$. Portanto,

$$c(a-b) = (d\lambda_1).(k\lambda_2) = mk\lambda_1,$$

ou seja, $ac \equiv bc(mod\ m)$. ■

Como consequência do teorema anterior, temos a lei do cancelamento para congruências, a qual no será bastante útil.

Corolário 5.8 ***(Lei do Cancelamento)*** *Suponhamos $ac \equiv bc(mod\ m)$, com $(c,m)=1$. Então, $a \equiv b(mod\ m)$.*

Demonstração: Se $ac \equiv bc(mod\ m)$, com $d=(c,m)=1$, então pelo teorema anterior, $a \equiv b(mod\ \frac{m}{d})$, isto é, $a \equiv b(mod\ m)$. ■

Proposição 5.9 *Sejam $a,k,m \in \mathbb{Z}$, com $m>1$ e $(k,m)=1$. Se $a_1,...,a_m$ é um sistema completo de resíduos módulo m, então*

$$a+ka_1,...,a+ka_m$$

também é um sistema completo de resíduos módulo m.

Demonstração: Como, do corolário acima, para $i,j = 0,1,...,m-1$, temos que

$$\begin{aligned} a+ka_i \equiv a+ka_j(mod\ m) &\Leftrightarrow ka_i \equiv ka_j(mod\ m) \\ &\Leftrightarrow a_i \equiv a_j(mod\ m) \\ &\Leftrightarrow i=j. \end{aligned}$$

Isso mostra que $a+ka_1,...,a+ka_m$ são, dois a dois, incongruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. ■

5.2 Congruências Lineares

Definição 5.3 *Dados a e b inteiros, com $a \neq 0$, uma congruência da forma*

$$ax \equiv b(mod\ m)$$

*é chamada **congruência linear**, em que x é uma incógnita.*

Nosso objetivo é determinar todas as soluções inteiras de $ax \equiv b(mod\ m)$, isto é, todos os inteiros x_0 para os quais

$$ax_0 \equiv b(mod\ m).$$

Por exemplo, x_0 é uma solução de $4x \equiv 7(mod\ 5)$, pois $4.3 = 12 \equiv 7(mod\ 5)$. Por outro lado, a congruência linear $4x \equiv 3(mod\ 2)$ não tem solução inteira, pois se $x_0 \in \mathbb{Z}$ e $4x_0 \equiv 3(mod\ 2)$, então $4x_0 - 3 = 2k$, com $k \in \mathbb{Z}$, de maneira que 2 divide 3, o que não é possível.

Inicialmente, vamos dar um critério para determinar se tais congruências, da forma como definidas acima, admitem solução.

Teorema 5.10 *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência linear $ax \equiv b(mod\ m)$ admite solução inteira se, e somente se, $d|b$, em que $d = (a,m)$.*

Demonstração: Suponhamos que x_0 seja solução de $ax \equiv b(mod\ m)$ e tomemos $d = (a,m)$. Assim, $ax_0 - b = km$, isto é $b = ax_0 - km$. Como, $d|a$ e $d|m$, então $d|b$.

Reciprocamente, suponha que $d|b$. Pela identidade de Bachet-Bézout, existem inteiros r e s tais que

$$d = a.r + s.m.$$

Como $b = dt$, com $t \in \mathbb{Z}$, $d|b$, então

$$b = (ar + sm)t = art + smt,$$

ou seja, $a(rt) \equiv b(mod\ m)$. Logo, $x_0 = rt$ é solução de $ax \equiv b(mod\ m)$. ■

Corolário 5.11 *A congruência $ax \equiv 1(mod\ m)$ tem solução se, e somente se, $(a,m) = 1$.*

A seguir vamos caracterizar as soluções de $ax \equiv b(mod\ m)$.

Teorema 5.12 *Se x_0 é uma solução da congruência linear $ax \equiv b(mod\ m)$, então todas as soluções desta congruência são da forma*

$$x = x_0 + \frac{m}{d}k, \ \ com \ \ k \in \mathbb{Z}$$

em que $d = (a,m)$.

Demonstração: Inicialmente, vamos provar que $x = x_0 + (\frac{m}{d})k$, com $d = (a,m)$, é uma solução de $ax \equiv b(mod\ m)$ para cada inteiro k. Desde que $ax_0 \equiv b(mod\ m)$, ou seja, $ax_0 = b + \lambda m$, com $\lambda \in \mathbb{Z}$, temos

$$ax = a[x_0 + (\frac{m}{d})k] = ax_0 + a(\frac{m}{d})k = b + m(\lambda + \frac{ak}{d}).$$

Portanto, $ax \equiv b(mod\ m)$, pois $\frac{ak}{d} \in \mathbb{Z}$.

Agora, seja $x_1 \in \mathbb{Z}$ tal que $ax_1 \equiv b(mod\ m)$. Como $ax_0 \equiv b(mod\ m)$, então, por transitividade, $ax_0 \equiv ax_1(mod\ m)$. Assim, pelo Teorema 5.7, $x_0 \equiv x_1(mod\ \frac{m}{d})$, ou seja,

$$x_1 = x_0 + \frac{m}{d}k, \ \ com \ \ k \in \mathbb{Z}.$$

■

Em particular,

Corolário 5.13 *A solução geral da congruência linear $ax \equiv 1(mod\ m)$ com, $(a,m) = 1$, é dada por*

$$x = x_0 + km, \ \ com \ \ k \in \mathbb{Z},$$

em que x_0 é uma solução inicial.

Existem soluções de $ax \equiv b(mod\ m)$ que são incongruentes duas a duas módulo m. Essas ocorrem em um número finito e são obtidas da expressão

$$x = x_0 + \frac{m}{d}k, \ \ para \ \ k = 0,1,...,d-1.$$

Vejamos no teorema a seguir.

Teorema 5.14 *Consideremos a congruência $ax \equiv b(mod\ m)$. Se $d|b$, com $d = (a,m)$, então esta congruência possui d soluções, duas a duas incongruentes módulo m, dadas por*

$$x_0, \ \ x_0 + \frac{m}{d}, \ \ x_0 + \frac{2m}{d}, ..., x_0 + \frac{(d-1)m}{d}, \tag{5.2}$$

em x_0 é uma solução particular qualquer de $ax \equiv b(mod\ m)$.

Demonstração: Pelo Teorema 5.12, para cada inteiro k,

$$x = x_0 + \frac{m}{d}k$$

é uma solução de $ax \equiv b(mod\ m)$. O que devemos mostrar é que

$$\left(x_0 + \frac{m}{d}k_1\right) \not\equiv \left(x_0 + \frac{m}{d}k_2\right)(mod\ m),$$

com $0 \leq k_1 < k_2 \leq d-1$. De fato, nestas condições, se

$$\left(x_0 + \frac{m}{d}k_1\right) \equiv \left(x_0 + \frac{m}{d}k_2\right)(mod\ m),$$

então

$$\frac{m}{d}k_1 \equiv \frac{m}{d}k_2(mod\ m),$$

e pelo Teorema 5.7,

$$k_1 \equiv k_2 (mod\ \frac{m}{d_1}),$$

sendo $d_1 = (\frac{m}{d}, m)$. Como $m = (\frac{m}{d})d$, então $d_1 = \frac{m}{d}$, de modo que

$$\frac{m}{d_1} = \frac{m}{\frac{m}{d}} = d.$$

Portanto, $k_1 \equiv k_2 (mod\ d)$, ou seja, $d|k_2 - k_1$, o que é uma contradição, desde que $0 < k_2 - k_1 < d - 1$. Por conseguinte, as soluções são duas a duas incongruentes módulo m.

Resta-nos mostrar que qualquer solução $x = x_0 + (\frac{m}{d})k$ de $ax \equiv b(mod\ m)$ é congruente módulo m a uma das d soluções dadas em (5.2). Pelo Algoritmo da Divisão, temos $k = dq + r$, com $0 \leq r \leq d - 1$. Assim,

$$\begin{aligned} x = x_0 + \frac{m}{d}k &= x_0 + \frac{m}{d}(dq + r) \\ &= x_0 + mq + r\frac{m}{d} \\ &\equiv x_0 + r\frac{m}{d} (mod\ m), \end{aligned}$$

em que $x_0 + r(\frac{m}{d})$ é uma das soluções em (5.2). ■

Resumindo os resultados anteriores, podemos resolver um congruência linear $ax \equiv b(mod\ m)$, com $d = (a, m)$ e $d|b$, seguindo os seguintes passos:

1. Através do Algoritmo de Euclides, obtemos inteiros r e s tais que

$$d = a.r + m.s.$$

2. Se $b = dt$, então $x_0 = rt$ é uma solução de $ax \equiv b(mod\ m)$, de modo que sua solução geral é dada por

$$x = x_0 + \frac{m}{d}k, \ \ com \ \ k \in \mathbb{Z}.$$

5.2.1 Sistemas de Congruências Lineares

No primeiro século da nossa era, o matemático chinês Sun-Tsu propôs o seguinte problema. *Qual é o número que deixa restos* 2, 3 *e* 2 *quando dividido, respectivamente, por* 3, 5 *e* 7*?*

A resposta dada por Sun-Tsu para esse problema foi 23. Em termos de congruências,

este problema consiste em resolver o seguinte sistema:

$$\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$$

De modo geral, estudaremos sistemas de congruências da forma:

$$\begin{cases} a_1 x & \equiv & b_1(mod\ m_1) \\ a_2 x & \equiv & b_2(mod\ m_2) \\ & \vdots & \\ a_k x & \equiv & b_k(mod\ m_k) \end{cases} \tag{5.3}$$

Para que este sistema tenha solução, é necessário que cada uma das k congruências tenha solução, ou seja, que $d_i|b_i$, em que $d_i = (a_i, m_i)$ para cada $i = 1, ..., k$. Entretanto, esta condição não é suficiente. Por exemplo, o sistema

$$\begin{cases} x \equiv 6(mod\ 4) \\ x \equiv 5(mod\ 2) \end{cases}$$

não possui solução, embora cada uma das congruências tenha solução.

O lema a seguir nos mostra como obter um sistema equivalente[1] ao dado em (5.3), mas com os coeficientes iguais a 1.

Lema 5.15 *A congruência linear $ax \equiv b(mod\ m)$, em que $d = (a, m)$, com $d|b$, é equivalente a*

$$x \equiv rb_1(mod\ n),$$

sendo $b = b_1 d$, $d = a.r + s.m$ e $m = nd$.

Demonstração: Considerando $a = a_1 d$, $b = b_1 d$ e $m = nd$,

$$ax \equiv b(mod\ m) \Leftrightarrow a_1 dx \equiv b_1 d(mod\ nd).$$

Pelo Teorema 5.7, temos

$$a_1 x \equiv b_1(mod\ n). \tag{5.4}$$

[1] Dois sistemas de congruências lineares são **equivalentes** quando possuem as mesmas soluções. O mesmo ocorre com duas congruências lineares.

Sendo $d = a.r + s.m$, então $d = a_1 d.r + s.nd$, ou seja, $1 = a_1.r + s.n$, isto é,

$$ra_1 \equiv 1(mod\ n).$$

Multiplicando a congruência em (5.4) por r, temos

$$ra_1 x \equiv rb_1(mod\ n),$$

e como $a_1 r \equiv 1(mod\ n)$, então $x \equiv a_1 rx(mod\ n)$, isto é,

$$x \equiv b_1 r(mod\ n),$$

o que prova a primeira parte.

Reciprocamente, se $x \equiv b_1 r(mod\ n)$, então como $ra_1 \equiv 1(mod\ n)$, segue $xra_1 \equiv b_1 r(mod\ n)$. Por outro lado, visto que $1 = a_1.r + s.n$, temos $(r,n) = 1$. Portanto, podemos cancelar o fator r da última congruência de modo a obter $xa_1 \equiv b_1(mod\ n)$, ou seja,

$$x\Big(\frac{a}{d}\Big) \equiv \frac{b}{d}\Big(mod\ \frac{m}{d}\Big),$$

donde $ax \equiv b(mod\ m)$. ■

A vantagem de se considerar uma congruência da forma $x \equiv b(mod\ m)$ é que sua solução geral é obtida de forma direta, $x = b + km$, com $k \in \mathbb{Z}$.

De acordo como o lema anterior, o sistema dado em (5.3) é equivalente ao sistema

$$\begin{cases} x & \equiv & c_1(mod\ n_1) \\ x & \equiv & c_2(mod\ n_2) \\ & \vdots & \\ x & \equiv & c_k(mod\ n_k) \end{cases} \tag{5.5}$$

o qual será resolvido através do teorema a seguir com uma hipótese adicional, cujo título faz lembrar a origem desse problema.

Teorema 5.16 ***(Teorema Chinês dos Restos)*** *Sejam $n_1, n_2, ..., n_k$ números naturais tais que $(n_i, n_j) = 1$ para $i \neq j$. Então, o sistema de congruências lineares dado em (5.5) possui uma solução, que é única módulo $n = n_1 n_2 ... n_k$.*

Demonstração: Sendo $n = n_1 n_2 ... n_k$, então

$$N_i = \frac{n}{n_i} = n_1 n_2 ... n_{i-1} n_{i+1} ... n_k,$$

ou seja, N_i é o produto de todos os inteiros $n_1 n_2 ... n_k$ excluindo n_i. Desde que $(n_i, n_j) = 1$

para $i \neq j$, então $(N_i, n_i) = 1$. Assim, pela identidade de Bachet-Bézout, existem inteiros r_i e s_i tais que

$$r_i N_i + s_i n_i = 1, \tag{5.6}$$

para cada $i = 1, ..., k$. Vamos provar que o inteiro

$$x_0 = \sum_{i=1}^{k} c_i r_i N_i = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k$$

é uma solução do sistema dado. Inicialmente, se $i \neq j$, então $N_j \equiv 0 (mod\ n_i)$, desde que $n_i | N_i$. Logo, $c_j r_j N_j \equiv 0 (mod\ n_i)$, de modo que

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k \equiv c_i r_i N_i (mod\ n_i).$$

Por outro lado, de (5.6), $r_i N_i \equiv 1 (mod\ n_i)$ para cada $i = 1, ..., k$. Daí, $c_i r_i N_i \equiv c_i (mod\ n_i)$ e, por transitividade, $x_0 \equiv c_i (mod\ n_i)$ para todo i. Isso mostra que x_0 é uma solução do sistema. Por fim, se y_0 é outra solução do sistema, então

$$y_0 \equiv c_i (mod\ n_i)$$

para cada $i = 1, ..., k$. Desse modo, $x_0 \equiv y_0 (mod\ n_i)$, isto é, $n_i | x_0 - y_0$. Desde que $(n_i, n_j) = 1$, com $i \neq j$, segue do Lema de Euclides que, $n = n_1 n_2 ... n_k$ divide $x_0 - y_0$, ou seja, $x_0 \equiv y_0 (mod\ n)$, o que prova a unicidade de solução módulo n. Por isso, a solução geral do sistema é

$$x = x_0 + kn, \ \ k \in \mathbb{Z}.$$

■

Exemplo 5.1 Determine a solução do sistema

$$\begin{cases} x & \equiv & 2 (mod\ 3) \\ x & \equiv & 3 (mod\ 5) \\ x & \equiv & 2 (mod\ 7) \end{cases}$$

usando o Teorema Chinês dos Restos.

Solução: Desde que $(3,5) = (3,7) = (5,7) = 1$, então podemos aplicar o **Teorema Chinês dos Restos**. Note que

$$n_1 = 3, \ \ n_2 = 5, \ \ n_3 = 7 \ \ e \ \ n = n_1 . n_2 . n_3 = 3.5.7 = 105$$

por outro lado,

$$N_1 = \frac{n}{n_1} = \frac{105}{3} = 35,\ \ N_2 = \frac{n}{n_2} = \frac{105}{5} = 21\ \ e\ \ N_3 = \frac{n}{n_3} = \frac{105}{7} = 15.$$

Agora, vamos determinar os inteiros r_i, s_i com $i = 1,2,3$ tais que, $r_i N_i + s_i n_i = 1$.

(i) $r_1 N_1 + s_1 n_1 = 1 \Rightarrow r_1.35 + s_1.12 = 1 \Rightarrow r_1 = -1\ \ e\ \ s_1 = 3.$

(ii) $r_2 N_2 + s_2 n_2 = 1 \Rightarrow r_2.21 + s_2.5 = 1 \Rightarrow r_2 = 1\ \ e\ \ s_2 = -4.$

(iii) $r_3 N_3 + s_3 n_3 = 1 \Rightarrow r_3.15 + s_3.7 = 1 \Rightarrow r_3 = 1\ \ e\ \ s_3 = -2.$

Como $c_1 = 2, c_2 = 3$ e $c_3 = 2$, então uma solução para o sistema pode ser dada por:

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + c_3 r_3 N_3 = 2.(-1).35 + 3.1.21 + 2.1.15 = 23.$$

Logo, a solução geral do sistema pode ser expressa da seguinte forma

$$x = 23 + 105t,\ \ t \in \mathbb{Z}.$$

▲

5.2.2 Equações Diofantinas Lineares

A denominação **equação diofantina** é uma homenagem a Diofanto de Alexandria, matemático grego do século III a.C. Diofanto viveu em uma importante cidade que era centro de atividades matemáticas da Grécia antiga. Não se sabe muito sobre a vida desse matemático. Em seu túmulo foram encontrados versos com problemas enigmáticos, pelos quais deduz-se que ele viveu 84 anos.

Enigma que, segundo dizem, teria sido gravada no túmulo de Diofanto por um amigo, Metrodorus, e cujo resultado revela a idade desse matemático:

> Viajante! Aqui estão as cinzas de Diofanto. É milagroso que os números possam medir a extensão da sua vida.
> Um sexto dela foi uma bela infância.
> Depois de $1/12$ da sua vida, a sua barba cresceu.
> Um sétimo da sua vida passou-se num casamento sem filhos.
> Mas, cinco anos após isso, nasceu o seu primeiro filho.
> Que viveu uma vida feliz durante apenas metade do tempo de vida do seu pai.
> E, em profundo pesar, o pobre velho terminou os seus dias na Terra, quatro anos após perder o seu filho, (Jornal de Mathemática Elementar nº 135).

Durante toda sua vida, Diofanto escreveu vários livros, entretanto o mais importante foi **Aritmética**. Neste livro, ele introduz uma notação simbólica com caracteres diferentes para o quadrado de uma incógnita, cubo de uma incógnita e assim sucessivamente. Neste

mesmo livro deu uma pequena introdução sobre as equações e hoje certas equações cujas soluções são números inteiros ou racionais são chamadas de Equações Diofantinas.

Definição 5.4 *Uma **equação diofantina linear** é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas.*

Uma equação da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

é chamada **equação diofantina linear**, em que $a_1, \ldots, a_n$ são inteiros dados, chamados **coeficientes**, c que também é um inteiro dado, é chamado **termo constante** e $x_1, ..., x_n$ são as **incógnitas**.

Teorema 5.17 *A equação diofantina $ax + by = c$ admite solução se, e somente se, (a,b) divide c.*

Demonstração: Suponha que a equação admita uma solução x_0, y_0. Então vale a igualdade $ax_0 + by_0 = c$. Como (a,b) divide a e divide b, então divide $ax_0 + by_0$, logo divide c.

Reciprocamente, suponha que (a,b) divida c, ou seja, $c = (a,b).d$, para algum inteiro d. Por outro lado, sabemos que existem inteiros r e s tais que

$$(a,b) = a.r + b.s.$$

Multiplicando ambos os lados da igualdade acima por d, obtemos

$$c = (a,b).d = a.(r.d) + b.(s.d).$$

Logo, a equação diofantina $ax + by = c$ admite pelo menos a solução

$$x = r.d \;\; e \;\; y = s.d.$$

■

Se a equação $ax + by = c$ admite uma solução, então o número $d = (a,b)$ divide c e, portanto, temos que $a = a'.d$, $b = b'.d$ e $c = c'.d$, onde $(a', b') = 1$.

Assim, é imediato verificar que x_0, y_0 é uma solução da equação $ax + by = c$ se, e somente se, é solução da equação $a'x + b'y = c'$, onde agora $(a', b') = 1$.

Portanto, toda equação diofantina linear que possui solução é equivalente a uma equação reduzida, ou seja, uma equação da forma

$$ax + by = c, \;\; com \;\; (a,b) = 1.$$

O próximo resultado nos dá uma fórmula para resolver a equação diofantinas linear $ax+by=c$, onde $(a,b)=1$, conhecida uma solução particular x_0, y_0 da equação.

Teorema 5.18 *Seja x_0, y_0 uma solução da equação $ax+by=c$, onde $(a,b)=1$. Então, as soluções x e y em $\mathbb{Z}$ da equação são*

$$x = x_0 + tb, \;\; y = y_0 - ta, \;\; t \in \mathbb{Z}.$$

Demonstração: Se x, y é uma solução qualquer da equação, então

$$ax + by = ax_0 + by_0 = c,$$

donde

$$a(x - x_0) = b(y_0 - y). \tag{5.7}$$

Daí segue que $a|b(y_0-y)$ e $b|a(x-x_0)$. Como $(a,b)=1$, $a|(y_0-y)$ e $b|(x-x_0)$. Assim,

$$y_0 - y = ta \;\; e \;\; x - x_0 = sb, \tag{5.8}$$

para alguns inteiros t e s. Substituindo esses valores em (5.7), obtemos

$$asb = bta,$$

o que implica que $s = t$. Logo, de (5.8), a solução é dada por

$$x = x_0 + tb, \;\; y = y_0 - ta, \;\; t \in \mathbb{Z}.$$

Reciprocamente, se $x = x_0 + tb \;\; e \;\; y = y_0 - ta$, substituindo esses valores na equação $ax+by=c$, obtemos

$$\begin{aligned} a(x_0 + bt) + b(y_0 - at) &= ax_0 + by_0 + abt - bat \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

■

Segue-se do teorema acima que a equação diofantina $ax+by=c$, com $(a,b)=1$, admite infinitas soluções em $\mathbb{Z}$.

Note também que as soluções da equação diofantina $ax+by=c$, podem ser escritas na forma $x = x_0 - tb$, $y = y_0 + ta$, $t \in \mathbb{Z}$, bastando para isso trocar t por $-t$ no Teorema 5.18.

Exemplo 5.2 Deseja-se comprar 225 bolas que são vendidas em caixas que contêm 6 ou 15 bolas. Determinar as quantidades necessárias de caixas para a efetivação da compra.

Solução: Considerando x e y os números de 6 e 15 bolas, respectivamente, o problema pode ser modelado na equação $6x+15=225$. Como $(6,15)=3$ e 3 divide 225, então esta equação tem solução inteira e, além disso, é equivalente à equação

$$2x+5y=75.$$

Por inspeção, uma solução particular para equação acima pode ser dada por $x_0=5$ e $y_0=13$. Logo, podemos escrever a solução geral da equação da seguinte forma:

$$\begin{cases} x &= x_0+bt \\ y &= y_0-at \end{cases} \Rightarrow \begin{cases} x &= 5+5t \\ y &= 13-2t \end{cases} ,t\in\mathbb{Z}.$$

Pela natureza do problema, apenas as soluções $x\geq 0$ e $y\geq 0$ são de interesse, então

$$\begin{cases} x &\geq 0 \\ y &\geq 0 \end{cases} \Rightarrow \begin{cases} 5+5t &\geq 0 \\ 13-2t &\geq 0 \end{cases} \Rightarrow \begin{cases} t &\geq -1 \\ t &\leq 6 \end{cases}$$

Portanto, $-1\leq t\leq 6$, ou seja, $t=\{-1,\ldots,6\}$ são os possíveis valores de t. Por exemplo, para $t=-1$, $x=0$ e $y=15$ (uma compra de 15 caixas com 15 bolas); $t=0$, $x=5$ e $y=13$ (uma compra de 5 caixas com 6 bolas e de 13 caixas com 15 bolas), e assim por diante. As outras possibilidades de compras são:

- para $t=1 \Rightarrow x=10$ e $y=11$,
- para $t=2 \Rightarrow x=15$ e $y=9$,
- para $t=3 \Rightarrow x=20$ e $y=7$,
- para $t=4 \Rightarrow x=25$ e $y=5$,
- para $t=5 \Rightarrow x=30$ e $y=3$,
- para $t=6 \Rightarrow x=35$ e $y=1$,

▲

O Teorema 5.17 pode ser estendido a equações diofantinas lineares com três ou mais variáveis e sua demonstração se faz por indução.

Teorema 5.19 *A equação diofantina linear $a_1x_1+a_2x_2+\cdots+a_nx_n=c$ possui solução se e, somente se $(a_1,\ldots,a_n)$ divide c.*

Exemplo 5.3 Verifique se a equação $6x+8y+12z=10$ tem solução e caso exista encontre sua solução geral.

Solução: Como $(6,8,12)=2$ e 2 divide 10 a equação possui solução. Como $8y+12z$ é uma combinação linear de 8 e 12, então deve ser um múltiplo de $4=(8,12)$, ou seja

$$8y+12z=4u \tag{5.9}$$

Assim, a equação original se reduz a $6x+4u=10$, que pelo Teorema 5.18 tem solução geral da forma $x=5+2t$, $u=-5-37$, com $t\in\mathbb{Z}$. Agora substituindo em (5.9) obtemos. $8y+12z=a(-5-3t)$, ou equivalentemente $2y+3z=-5-3t$.

Agora observe que

$$1=(2,3)=2.2-1.3 \;\Rightarrow\; -(10+6t).2+(5+3t).3=-5-3t$$

o que nos dá uma solução particular e daí a solução geral é

$$y=-10-6t+3t' \quad \text{e} \quad z=5+3t-2t'.$$

Portanto, a solução geral da equação original é

$$\begin{cases} x &= 5+2t \\ y &= -10-6t+3t' \\ z &= 5+3t-2t', \end{cases}$$

com $t,t'\in\mathbb{Z}$. ▲

Observação: O método acima pode ser aplicado a uma equação diofantina com um número qualquer de variável.

5.3 Os Teoremas de Wilson, Fermat e Euler

5.3.1 Teorema de Wilson

Nesta seção, vamos provar um teorema atribuído a Wilson $(1741-1793)$, mas que, na realidade, foi provado, pela primeira vez, por J. L. Lagrange[2] $(1736-1813)$. Antes de

[2]Joseph Louis Lagrange (Turim, 25 de janeiro de 1736-Paris, 10 de abril de 1813) foi um matemático italiano. Organizou as pesquisas desenvolvidas pelos associados da Academia de Ciências de Turim. O primeiro volume das memórias da academia foi publicado em 1759, quando Lagrange tinha vinte e três anos, aplicou o cálculo diferencial à teoria da probabilidade, indo além de **Isaac Newton** com um novo começo na teoria matemática do som.

apresentar uma prova desse teorema, vamos demonstrar dois lemas que nos auxiliarão nesta demonstração.

Lema 5.20 *Seja p um número primo. Então, as únicas soluções módulo p da congruência $a^2 \equiv 1(mod\ p)$ são 1 e -1.*

Demonstração: Se x_0 é uma solução da congruência $a^2 \equiv 1(mod\ p)$, então $x_0^2 \equiv 1(mod\ p)$, ou seja,

$$p|x_0^2 - 1 = (x_0 + 1)(x_0 - 1).$$

Como p é primo, segue que $p|(x_0 + 1)$ ou $p|(x_0 - 1)$. Por conseguinte, $x_0 \equiv -1 \equiv (p - 1)(mod\ p)$ ou $x_0 \equiv 1(mod\ p)$. ■

Lema 5.21 *Sejam p um número primo e $A = \{1, 2, \ldots, p-1\}$. Então, para cada $a \in A$, existe único $b \in A$ tal que $ab \equiv 1(mod\ p)$.*

Demonstração:
(Existência) Dado $a \in A$, $(a, p) = 1$, de modo que, pela identidade de Bachet-Bézout, existem inteiros r e s tais que $1 = ar + ps$, isto é, $ar \equiv 1(mod\ p)$. Como $r \not\equiv 0(mod\ p)$, pois p$\nmid$ 1, temos $r \equiv b(mod\ p)$ para algum $b \in A$. Assim, $ar \equiv ab(mod\ p)$ e, por transitividade, $ab \equiv 1(mod\ p)$, provando a existência de $b \in A$.
(Unicidade) Se b_1 e b_2 são elementos de A, com $ab_1 \equiv 1(mod\ p)$ e $ab_2 \equiv 1(mod\ p)$, então $ab_2 \equiv ab_1(mod\ p)$. Como $(a, p) = 1$, temos $b_2 \equiv b_1(mod\ p)$. Isso mostra a unicidade do elemento b módulo p. ■

Teorema 5.22 ***(Teorema de Wilson)*** *Um número natural p é primo se, e somente se,*

$$(p-1)! \equiv -1(mod\ p).$$

Demonstração: Suponhamos que $(p-1)! \equiv -1(mod\ p)$. Se p é composto, então $p = m.n$, com $1 < n < p$, de modo que

$$(p-1)! \equiv -1(mod\ p) \Rightarrow (p-1)! \equiv -1(mod\ n).$$

Como $1 < n \leq p - 1$, então $n|(p-1)!$, isto é, $(p-1)! \equiv 0(mod\ n)$. Assim, por transitividade, $-1 \equiv 0(mod\ n)$, ou seja, $n|1$, o que é uma contradição. Logo, p é primo.

Reciprocamente, Seja p um número primo. Se $p = 2$ ou $p = 3$, o resultado segue imediatamente. Por isso, vamos supor que $p > 3$. De acordo com os Lemas 5.20 e 5.21, podemos agrupar os números

$$2, 3, \ldots, p-2$$

em $\frac{(p-3)}{2}$ pares a e b tais que $ab \equiv 1(mod\ p)$. Por conseguinte, multiplicando todas essas congruências membro a membro, obtemos que

$$2.3\ldots(p-2) \equiv 1(mod\ p).$$

Considerando que $(p-1) \equiv -1(mod\ p)$, então, multiplicando membro a membro estas duas congruências, $2.3\ldots(p-2)(p-1) \equiv -1(mod\ p)$, ou seja,

$$(p-1)! \equiv -1(mod\ p).$$

■

Exemplo 5.4 Determinar o resto da divisão de $2(26)!$ por 29.

Solução: Como $p = 29$ é primo, então pelo Teorema de Wilson, temos que $28! \equiv -1(mod\ 29)$, ou melhor, $28.27.26! \equiv -1(mod\ 29)$. Por outro lado, sendo $28 \equiv -1(mod\ 29)$ e $27 \equiv -2(mod\ 29)$,

$$28.27 \equiv 2(mod\ 29)$$

e, por conseguinte, $28.27.26! \equiv 2.26!(mod\ 29)$. Desse modo, por transitividade,

$$2.26! \equiv -1 \equiv 28(mod\ 29).$$

Portanto, o resto é $r = 28$. ▲

5.3.2 O Pequeno Teorema de Fermat

Desde, pelo menos, 50 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então, $p|2^p - 2$. Coube a Pierre de Fermat, no século XVII, generalizar esse resultado, enunciando um pequeno, mas notável, teorema. O resultado de Pierre de Fermat, conhecido como **Pequeno Teorema de Fermat**, pode ser assim enunciado: e

Teorema 5.23 ***(Pequeno Teorema de Fermat)*** *Sejam p um primo e a um inteiro tal que $p \nmid a$. Então,*

$$a^{p-1} \equiv 1(mod\ p).$$

Demonstração: Consideremos os primeiros $p-1$ múltiplos de a, ou seja,

$$a, 2a, 3a, \ldots, (p-1)a. \tag{5.10}$$

Observemos primeiramente que estes números são dois a dois incongruentes módulo p. De fato, se

$$ak_1 \equiv ak_2 (mod\ p),$$

com $1 \leq k_1 < k_2 \leq p-1$, então como $(a,p) = 1$, segue do Corolário 5.8 que $k_1 \equiv k_2 (mod\ p)$, isto é, $p|k_2 - k_1$, o que é impossível. Além disso, se $1 \leq r \leq p-1$ e $p|ra$, então $p|a$ ou $p|r$, o que também não é possível. Portanto, $ra \not\equiv 0 (mod\ p)$ para todo $r = 1, \ldots, p-1$.

De acordo com o Algoritmo da Divisão, cada inteiro é congruente módulo p a um, e somente um, número da sequência

$$1, 2, 3, \ldots, p-1. \tag{5.11}$$

Portanto, cada inteiro de (5.10) é equivalente a um número de (5.11) numa determinada ordem, digamos

$$\begin{aligned} a &\equiv b_1 (mod\ p), \\ 2a &\equiv b_2 (mod\ p), \\ &\vdots \\ (p-1)a &\equiv b_{p-1} (mod\ p), \end{aligned}$$

em que $b_i \in \{1, 2, \ldots, p-1\}$ para $i = 1, 2, \ldots, p-1$. Multiplicando membro a membro estas congruências, temos que

$$a.2a \ldots (p-1)a \equiv 1.2 \ldots (p-1) (mod\ p),$$

isto é,

$$a^{p-1}(p-1)! \equiv (p-1)! (mod\ p).$$

Como $((p-1)!, p) = 1$, podemos cancelar $(p-1)!$ desta última congruência, de modo que

$$a^{p-1} \equiv 1 (mod\ p).$$

■

O resultado anterior implica que para um inteiro a qualquer, divisível por p ou não, $a^p \equiv a (mod\ p)$. Com efeito,

Corolário 5.24 *Se p é primo, então*

$$a^p \equiv a (mod\ p)$$

para qualquer inteiro a.

Demonstração: Se $p \nmid a$, então pelo teorema anterior, $a^{p-1} \equiv 1(mod\ p)$. Assim, multiplicando esta congruência por a, segue que $a^p \equiv a(mod\ p)$. Se $p|a$, então $p|a^p$ e, por isso, $p|a^p - a$, ou seja, $a^p \equiv a(mod\ p)$. ■

Note que o Pequeno Teorema de Fermat fornece-nos um teste de não Primalidade. De fato, dado $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a,m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m não é primo.

Exemplo 5.5 Determinar o resto da divisão de 2^{2017} por 7.

Solução: Considerando $p = 7$ e $a = 2$, temos que $p \nmid a$. Assim, pelo Pequeno Teorema de Fermat,

$$2^6 \equiv 1(mod\ 7).$$

Elevando ambos os membros desta congruência 288 ($2017 = 7.288 + 1$), obtemos

$$2^{2016} \equiv 1(mod\ 7).$$

Multiplicando esta congruência por 2,

$$2^{2017} \equiv 2(mod\ 7).$$

Logo, o resto da divisão é $r = 2$. ▲

5.3.3 Teorema de Euler

O **Teorema de Euler** é uma generalização do Pequeno Teorema de Fermat, no sentido de considerar congruência módulo m, em que m pode ser primo ou não. Vamos iniciar esta seção apresentando a definição da Função φ de Euler, a qual é parte central desse teorema.

Definição 5.5 *Para cada $m > 1$, seja $\varphi(m)$ a quantidade de números inteiros b, $1 \leq b < m$, tais que $(m,b) = 1$. Isso define uma importante função,*

$$\varphi : \mathbb{N} \to \mathbb{N},$$

*chamada **função φ (fi) de Euler.***

Pela definição anterior, temos que

$$\varphi \leq m - 1, \text{ para todo } m \geq 2.$$

Além do mais, se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um número primo. Os resultados a seguir serão úteis para determinarmos uma expressão para $\varphi(m)$.

Teorema 5.25 *Se p é primo e $k \geq 1$, então*

$$\varphi(p^k) = p^k - p^{k-1} = p^k\Big(1 - \frac{1}{p}\Big).$$

Demonstração: Inicialmente, note que $(m, p^k) = 1$ se, e somente se, $p \nmid m$. Agora, entre 1 e p^k existem p^{k-1} números que são divisíveis por p, a saber

$$p, 2p, 3p, \ldots, (p^{k-1})p,$$

pois $p\lambda \leq p^k$ se, e somente se, $\lambda = 1, 2, \ldots, p^{k-1}$. Desse modo, o conjunto $\{1, 2, \ldots, p^k\}$ contém exatamente $p^k - p^{k-1}$ números que são relativamente primos com p^k. Daí, por definição,

$$\varphi(p^k) = p^k - p^{k-1} = p^k\Big(1 - \frac{1}{p}\Big).$$

■

Definição 5.6 *Um **sistema reduzido de resíduos** módulo m é um conjunto de números inteiros $r_1, \ldots, r_s$ tais que*

(i) $(r_i, m) = 1$, para todo $i = 1, \ldots, s$;

(ii) $r_i \not\equiv r_j (mod\ m)$, se $i \neq j$;

(iii) Para cada $n \in \mathbb{Z}$ tal que $(n, m) = 1$, existe i tal que $n \equiv r_i (mod\ m)$.

Pode-se obter um sistema reduzido de resíduos módulo m a partir de um sistema completo qualquer de resíduos $a_1, \ldots a_m$ módulo m, bastando para isso eliminar do sistema completo de resíduos todos os elementos que não são primos com m. De fato, as propriedades (i) e (ii) da definição são claramente verificadas para $r_i, \ldots, r_s$. Por outro lado, dado um número inteiro n, existe j que $n \equiv a_j (mod\ m)$. Se $(n, m) = 1$, então, $(a_j, m) = 1$, e portanto, para algum j, temos que $a_j = r_i$ e, consequentemente, $n \equiv r_i (mod\ m)$.

Vamos designar por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Note ainda que dois sistemas reduzidos de resíduos módulo m têm o mesmo número de elementos.

Proposição 5.26 *Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $(a, m) = 1$. Então, $ar_1, \ldots, ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração: Seja $a_1, \ldots, a_m$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido de resíduos $r_1, \ldots, r_{\varphi(m)}$. Do fato de que $(a, m) = 1$, tem-se que $(a_i, m) = 1$ se, e somente se, $(aa_i, m) = 1$, o resultado segue. ■

Teorema 5.27 *A função φ de Euler é multiplicativa, isto é, se m e n são números naturais tais $(m,n)=1$, então*

$$\varphi(mn)=\varphi(m)\varphi(n).$$

Demonstração: O resultado é imediato se $m=1$ ou $n=1$. Portanto, vamos supor que $m>1$ e $n>1$. Vamos considerar a tabela formada pelos inteiros de 1 a *mn*, dada como segue:

$$\begin{array}{lrcrcr}
1 & 2 & \ldots & r & \ldots & m \\
m+1 & m+2 & \ldots & m+r & \ldots & 2m \\
2\text{m+1} & 2m+2 & \ldots & 2m+r & \ldots & 3m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+r & \ldots & nm
\end{array}$$

Como se tem que $(t,mn)=1$ se, e somente se, $(t,n)=(t,m)=1$, para calcular $\varphi(mn)$, devemos determinar os inteiros na tabela acima que são simultaneamente primos com *m* e *n*.

Se o primeiro elemento de uma coluna não for primo com *n*, então todos os elementos da coluna não são primos com *n*. Portanto, os elementos primos com *n* estão necessariamente nas colunas restantes que são em número $\varphi(n)$, cujos elementos são primos com *n*. Vejamos agora quais são os elementos primos com *m* em cada uma dessas colunas.

Como $(m,n)=1$, a sequência

$$k, n+k, \ldots, (m-1)n+k$$

forma um sistema completo de resíduos módulo *m* e, portanto, $\varphi(m)$ desses elementos são primos com *m*. logo, o número de elementos simultaneamente primos com *n* e *m* é $\varphi(m)\varphi(n)$.

■

O próximo resultado nos mostra como calcular $\varphi(n)$.

Teorema 5.28 *Se $m=p_1^{r_1}\ldots p_k^{r_k}$ é uma decomposição de m em fatores primos, então,*

$$\varphi(m)=m\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_1}\Big)\ldots\Big(1-\frac{1}{p_k}\Big).$$

Demonstração: Pelo Teorema 5.26, temos

$$\varphi(p_i^{r_i})=p_i^{r_i}-p_i^{r_i-1}=p_i^{r_i}\Big(1-\frac{1}{p_i}\Big).$$

Portanto, o Teorema 5.28 nos garante que

$$\begin{aligned}\varphi(p_1^{r_1}\dots p_k^{r_k}) &= p_1^{r_1}\Big(1-\frac{1}{p_1}\Big)p_2^{r_2}\Big(1-\frac{1}{p_2}\Big)\dots p_k^{r_k}\Big(1-\frac{1}{p_k}\Big)\\ &= p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\dots\Big(1-\frac{1}{p_k}\Big)\\ &= m\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_1}\Big)\dots\Big(1-\frac{1}{p_k}\Big).\end{aligned}$$

■

A fórmula do teorema anterior pode ser reescrita da seguinte maneira:

$$\varphi(p_1^{r_1}\dots p_k^{r_k}) = p_1^{r_1-1}(p_1-1)\dots(p_k-1).$$

Exemplo 5.6 Calcular $\varphi(1008)$.

Solução: Como $1008 = 2^4.3^2.7$,

$$\begin{aligned}\varphi(1008) = \varphi(2^4.3^2.7) &= \varphi(2^4)\varphi(3^2)\varphi(7)\\ &= (2^4-2^3)(3^2-3)(7-1)\\ &= 8.6.6\\ &= 288.\end{aligned}$$

Usando o Teorema 5.29, com $m = 1008$, $p_1 = 2$, $p_2 = 3$ e $p_3 = 7$, segue que

$$\begin{aligned}\varphi(1008) &= \Big(1-\frac{1}{2}\Big)\Big(1-\frac{1}{3}\Big)\Big(1-\frac{1}{7}\Big)\\ &= 1008\Big(\frac{1}{2}\Big)\Big(\frac{2}{3}\Big)\Big(\frac{6}{7}\Big)\\ &= 288.\end{aligned}$$

▲

Teorema 5.29 *Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $(a,m) = 1$. Então,*

$$a^{\varphi(m)} \equiv 1 (mod\ m).$$

Demonstração: Seja $\{r_1,\dots,r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Logo, pela Proposição (5.27), $\{ar_1,\dots,ar_{\varphi(m)}\}$ formam um sistema reduzido de resíduos módulo m e, portanto,

$$ar_1.ar_2\dots,ar_{\varphi(m)} \equiv r_1.r_2\dots r_{\varphi(m)} (mod\ m).$$

Consequentemente,

$$a^{\varphi(m)} r_1.r_2 \dots r_{\varphi(m)} = ar_1.ar_2 \dots ar_{\varphi(m)} \equiv r_1.r_2 \dots r_{\varphi(m)} (mod\ m).$$

Como $(r_1.r_2 \dots r_{\varphi(m)}, m) = 1$, é válida a lei do cancelamento com relação à multiplicação e, então,

$$a^{\varphi(m)} \equiv 1 (mod\ m).$$

■

Exemplo 5.7 Determinar o resto da divisão de 3^{2017} por 8.

Solução: Como $(3,8) = 1$, podemos aplicar o Teorema de Euler considerando $a = 3$ e $m = 8$. Fazendo isso, como $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$,

$$3^4 \equiv 1 (mod\ 8).$$

Elevando ambos os membros desta congruência a 504 ($2017 = 4.504 + 1$), obtemos que $3^{2016} \equiv 1 (mod\ 8)$. Logo, $3^{2017} \equiv 3 (mod\ 8)$ e, portanto, o resto procurado é $r = 3$. ▲

Capítulo 6

Teoremas da Aritmética na Resolução de Problemas Olímpicos

Como William Timothy Gowers escreveu em seu livro de divulgação *A Short Introduction to Mathematics (Uma breve introdução à Matemática)* e Carlos Yuzo Sbine traduziu em seu livro 21 *Aulas de Matemática Olímpica*:

> Muitas vezes a beleza da Matemática se compara à beleza da música: muitas vezes gostamos de uma música porque de repente ela muda sutilmente e essa pequena mudança nos leva a caminhos totalmente novos e inesperados. Isso faz com que músicas novas sejam compostas. Da mesma forma, uma ideia Matemática um pouquinho só diferente pode nos levar a lugares que nem imaginamos. É por isso que, assim como a música, a Matemática nunca cessa: sempre alguém inventa algo novo que é belo e inesperado, (SBINE, Carlos Yuzo).

Neste ponto, as Olimpíadas de Matemática têm um papel importante: elas proporcionam aos estudantes uma fantástica oportunidade de conhecer uma Matemática diferente, com pequenas novas ideias que levam a um grande e novo mundo de conhecimento.

De acordo com análise feita em provas de edições anteriores, as Olimpíadas de Matemática trazem muitos problemas de aritmética. Neste sentido, apresentamos agora alguns problemas envolvendo divisibilidade e congruência modular, com o objetivo de proporcionar a atração e despertar a curiosidade de professores e alunos pela Matemática, além de constituir um aprendizado mais formal dos conceitos que possibilitam a resolução dos problemas propostos.

Os problemas apresentados neste capítulo foram extraídos da OBM, OBMEP e OCM, edição anteriores, além do Banco de Questões 2017 da OBMEP e do material elaborado pelo programa *Polos Olímpicos de Treinamento Intensivo (POTI)*[1]. O critério de seleção usado, na escolha dos problemas foi a aplicação direta das propriedades, dos conceitos e dos teoremas da aritmética apresentados nos capítulos anteriores.

[1] O programa é destinado para cursos de Treinamento Intensivo voltados para competições de matemática. A finalidade principal dessa iniciativa é melhorar o desempenho dos alunos brasileiros nas olimpíadas OBMEP e OBM através do financiamento de aulas presenciais em polos que apresentem demanda e estrutura adequada para tal.

Problema 6.1 ***(OBM 2015 - N2, Segunda Fase)*** *Determine o número de inteiros positivos n menores que 100 de modo que a fração*

$$\frac{8n+5}{5n+8} \tag{6.1}$$

não seja irredutível.

Solução 6.1 *Seja $d = (5n+8, 8n+5)$ então $d|5n+8$ e $d|8n+5$. Para que a fração $\frac{8n+5}{5n+8}$ não seja irredutível, devemos ter $d \neq 1$. Aplicando o* ***Lema de Euclides****, temos*

$$\begin{aligned}
(5n+8, 8n+5) &= (5n+8, 8n+5-(5n+8)) \\
&= (5n+8, 3n-3) \\
&= (3n-3, 5n+8-(3n-3)) \\
&= (3n-3, 2n+11) \\
&= (2n+11, 3n-3-(2n+11)) \\
&= (2n+11, n-14) \\
&= (n-14, 2n+11-(n-14)) \\
&= (n-14, n+25) \\
&= (n-14, n+25-(n-14)) \\
&= (n-14, 39).
\end{aligned}$$

Como $39 = 3.13$ basta determinar os múltiplos de 3 e 13 tais que

$$\left\{ \begin{array}{rcl} n-14 & \equiv & 0 (mod\ 3) \\ n-14 & \equiv & 0 (mod\ 13) \end{array} \right. \Rightarrow \left\{ \begin{array}{rcl} n & \equiv & 14 (mod\ 3) \\ n & \equiv & 14 (mod\ 13) \end{array} \right. \Rightarrow \left\{ \begin{array}{rcl} n & \equiv & 2 (mod\ 3) \\ n & \equiv & 1 (mod\ 13) \end{array} \right.$$

ou seja, devemos encontrar os números inteiros positivos menores que 100 que deixam resto 2 quando divididos por 3 e deixam resto 1 quando divididos por 13.

(i) Conjunto dos números inteiros positivos menores que 100 que deixam resto 2 quando divididos por 3.

$$\{2, 5, 8, \ldots, 92, 98\}$$

que possui $\frac{98-2}{3} + 1 = 33$ números.

(ii) Conjunto dos números inteiros positivos menores que 100 que deixam resto 1 quando divididos por 13.

$$\{1, 14, 27, \ldots, 79, 92\}$$

que possui $\frac{92-1}{13} + 1 = 8$ números.

No entanto, observe que os números 14, 53 *e* 92 *figuram em ambos os conjuntos, portanto existem* $33+8-3=38$ *números inteiros e positivos menores que* 100 *que tornam a fração em* (6.1) *redutível, ou seja,* $d \neq 1$. ■

Problema 6.2 ***(OBM 2016 - N2, Primeira Fase)*** *O número de seis dígitos* $ab2016$ *na base* 10 *é múltiplo de* 99. *Determine o valor do dígito a.*

Solução 6.2 *Inicialmente note que* $99 = 3^2.11$, *ou seja, um múltiplo de* 99 *também é múltiplo de* 9 *e* 11. *Pelo critério de divisibilidade por* 11, *para que* $ab2016$ *seja divisível por* 11, *devemos ter*

$$11|(a+2+1)-(b+0+6) = a-b-3.$$

Além disso, para que o número dado seja divisível por 9, *devemos ter*

$$9|a+b+2+0+1+6 = a+b+9.$$

Pela relação de dividibilidade anterior, podemos ter $a+b=9$ *ou* $a+b=18$. *No primeiro caso, temos*

$$11|a-b-3 = 2(3-b).$$

O único dígito que satisfaz a relação anterior é $b=3$. *Consequentemente,* $b=6$. *No segundo caso,* $a=b=9$ *e* $11|9-9-3=-3$. *Isso é um absurdo e a única solução possível é* $(a,b)=(6,3)$. ■

Problema 6.3 ***(OBM 2016 - N2, Primeira fase)*** *Determine o menor inteiro positivo n tal que* $n!$ *é múltiplo de* 2016.

Solução 6.3 *Fatorando* 2016 *em primos, obtemos* $2016 = 2^5.3^2.7$. *Assim,* $n!$ *deve conter pelo menos essas potências de primos como seus divisores. Para que apareça o fator* 7 *na fatoração de* $n!$, *devemos ter* $n \geq 7$. *Como* 2^5 *não divide* $7! = 540$, *o próximo candidato é* $8! = 40320 = 20.2016$. *Portanto, o menor valor de n é* 8. ■

Problema 6.4 ***(OBMEP 2017 - N3, Primeira Fase)*** *Somando* 1 *a um certo número natural, obtemos um múltiplo de* 11. *Subtraindo* 1 *desse mesmo número, obtemos um múltiplo de* 8. *Qual é o resto da divisão do quadrado desse número por* 88*?*

A) 0 *B)* 1 *C)* 8 *D)* 10 *E)* 80

Solução 6.4 *Seja x um número natural. Analisando os dados disponíveis no enunciado do problema, podemos montar o seguinte sistema.*

$$\begin{cases} x \equiv -1 (mod\ 11) \quad (I) \\ x \equiv 1 (mod\ 8) \quad (II) \end{cases}$$

Das equações (I) *e* (II)*, obtemos*

$$x = 11a - 1 \Rightarrow 11a - 1 \equiv 1 (mod\ 8) \Rightarrow 11a \equiv 2 (mod\ 8),\ a \in \mathbb{Z}$$

Pelo Teorema 5.7 *obtemos*

$$3.11a \equiv 3.2 (mod\ 8) \Rightarrow 33a \equiv 6 (mod\ 8) \Rightarrow a \equiv 6 (mod\ 8). \tag{6.2}$$

De forma equivalente, podemos escrever (6.2) *como*

$$a = 8b + 6,\ \ b \in \mathbb{N}. \tag{6.3}$$

Assim, substituindo (6.3) *na equação* $x = 11a - 1$ *e utilizando as propriedades de congruência, obtemos*

$$\begin{aligned} x = 11a - 1 &\Rightarrow x = 11(8b + 6) - 1 \\ &\Rightarrow x = 88c + 65,\ \ c \in \mathbb{N} \\ &\Rightarrow x \equiv 65 (mod\ 88) \\ &\Rightarrow x \equiv -23 (mod\ 88) \\ &\Rightarrow x^2 \equiv 529 (mod\ 88) \\ &\Rightarrow x^2 \equiv 1 (mod\ 88). \end{aligned}$$

Portanto, o resto procurado é igual a 1*. Um solução alternativa para esse problema pode ser obtida aplicando o* ***Teorema Chinês dos Restos****.* ■

Problema 6.5 ***(OBMEP 2017 - N3, Primeira Fase)*** *A maior potência de* 2 *que divide o produto* $1.2 \ldots 2023.2024$ *é* 2^{2017}*. Qual a maior potência de* 2 *que divide o produto* $1.2 \ldots 4047.4048$*?*

A) 2^{2018} *B)* 2^{4034} *C)* 2^{4041} *D)* 2^{6051} *E)* 2^{8068}

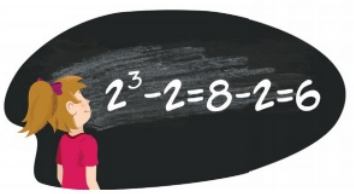
Solução 6.5 *Pelos dados disponíveis no enunciado do problema, a maior potência de* 2 *que divide o produto* $1.2 \ldots 2023.2024 = 2024!$ *é* 2^{2017}*. Nosso objetivo é determinar a maior potência de* 2 *que divide o seguinte produto* $1.2 \ldots 4047.4048 = 4048!$*.*

Pelo ***Teorema de Legendre****, temos que*

$$\begin{aligned} E_2[4048!] &= \left[\frac{4048}{2}\right]+\left[\frac{4048}{2^2}\right]+\left[\frac{4048}{2^3}\right]+\cdots+\left[\frac{4048}{2^9}\right]+\left[\frac{4048}{2^{10}}\right]+\left[\frac{4048}{2^{11}}\right] \\ &= 2024+1012+506+\cdots+7+3+1 \\ &= 4041. \end{aligned}$$

Portanto, a maior potência de 2 *que divide* 4048! *é* 2^{4041}. ■

Problema 6.6 ***(OBMEP 2017 - N2, Segunda fase)*** *Júlia faz o seguinte cálculo com números positivos: ela escolhe um número, eleva esse número ao cubo e subtrai desse cubo o próprio número. Veja na figura que o resultado do cálculo de Júlia com o número* 2 *é igual a* 6*.*



(a) Qual é o resultado do cálculo de Júlia com o número 3?

(b) Qual é o número que deve ser escolhido por Júlia para que o resultado do cálculo seja 1320*?*

(c) Explique por que, para qualquer número que Júlia escolher, o resultado final do cálculo será sempre um múltiplo de 6*.*

Solução 6.6 *(a) Para efetuar o cálculo com o número* 3*, vamos adotar o mesmo procedimento feito por Júlia com o número* 2*. Ou seja,*

$$3^3-3=27-3=24.$$

(b) Seja x o número escolhido por Júlia. Assim,

$$\begin{aligned} x^3-x=1320 &\Rightarrow x(x^2-1)=1320 \\ &\Rightarrow x(x-1)(x+1)=1320 \\ &\Rightarrow (x-1)x(x+1)=2^3.3.5.11. \end{aligned}$$

Observe que $(x-1)$*,* x *e* $(x+1)$ *são números consecutivos, então organizando a fatoração em números primos de* 1320*, obtemos*

$$(x-1)x(x+1)=2.5.11.3.4 \Rightarrow (x-1)x(x+1)=10.11.12.$$

Portanto, o número que Júlia deve escolher é 11.

(c) Seja x um números inteiro positivo. Pelo item (b) temos que $x^3 - x = (x-1)x(x+1)$ *é o produto de três números inteiros e consecutivos. Neste caso, para provar que* $x^3 - x$ *é múltiplo de* 6*, basta mostrar que* $x^3 - x$ *é múltiplo de* 3 *e* 2*.*

(I) existe um múltiplo de 3 *entre* $(x-1)$*,* x *ou* $(x+1)$*.*

De fato, sendo $(x-1)$*,* x *e* $(x+1)$ *números inteiros consecutivos. Pelo* ***Algoritmo de Euclides****,*

$$x - 1 = 3q + r, \;\; 0 \leq r \leq 2.$$

Daí, temos 3 *casos para analisarmos.*

(i) Se $r = 0$*, então* $x - 1 = 3q$*,* $x = 3q - 1$ *e* $x + 1 = 3q + 1$*,* $q \in \mathbb{Z}$*. Neste caso,* $x - 1 = 3q$ *é o único múltiplo de* 3 *dentre* $(x-1)$*,* x *e* $(x+1)$*.*

(ii) Se $r = 1$*, então* $x - 1 = 3q$*,* $x = 3q + 1$ *e* $x + 1 = 3q + 2$*,* $q \in \mathbb{Z}$*. Neste caso,* $x - 1 = 3q$ *é o único múltiplo de* 3 *dentre* $(x-1)$*,* x *e* $(x+1)$*.*

(iii) Se $r = 2$*, então* $x - 1 = 3q + 1$*,* $x = 3q + 1$ *e* $x + 1 = 3q + 3 = 3(q+1)$*,* $q \in \mathbb{Z}$*. Neste caso,* $x + 1 = 3(q+1)$ *é o único múltiplo de* 3 *dentre* $(x-1)$*,* x *e* $(x+1)$*.*

Logo, para $0 \leq r \leq 2$ *existe um múltiplo de* 3 *entre* $x - 1 = 3q - 1$*,* $x = 3q$ *e* $x + 1 = 3q + 1$*.*

(II) existe um múltiplo de 2 *entre* $(x-1)$*,* x *ou* $(x+1)$*.*

Seja $(x-1)$*,* x *e* $(x+1)$ *números inteiros consecutivos. Pelo* ***Algoritmo de Euclides****, temos que*

$$x - 1 = 2q + r, \;\; 0 \leq r \leq 1.$$

Daí, temos 2 *casos para analisarmos.*

(i) Se $r = 0$*, então* $x - 1 = 2q$*,* $x = 2q + 1$ *e* $x + 1 = 2q + 2 = 2(q+1)$*,* $q \in \mathbb{Z}$*. Neste caso,* $x - 1 = 2q$ *e* $x + 1 = 2(q+1)$ *são múltiplos de* 2 *dentre* $(x-1)$*,* x *e* $(x+1)$*.*

(ii) Se $r = 1$*, então* $x - 1 = 2q + 1$*,* $x = 2q + 2 = 2(q+1)$ *e* $x + 1 = 2q + 3$*,* $q \in \mathbb{Z}$*. Neste caso,* $x = 2q$ *é o único múltiplo de* 2 *dentre* $(x-1)$*,* x *e* $(x+1)$*.*

Portanto, para $0 \leq r \leq 1$ *existe um múltiplo de* 2 *entre* $x - 1 = 2q - 1$*,* $x = 2q$ *e* $x + 1 = 2q + 1$*.*

Assim concluímos que $x^3 - x$ *é múltiplo de* 6 *para qualquer número escolhido por Júlia.* ■

Problema 6.7 ***(Banco de Questões OBMEP - 2017, pg.*** 93***)*** *Determine se o número*

$$\underbrace{11\ldots1}_{2016}2\underbrace{11\ldots1}_{2016}$$

é um número primo ou um número composto.

Solução 6.7 *Inicialmente, vamos representar o número*

$$\underbrace{11\ldots1}_{2016}2\underbrace{11\ldots1}_{2016}$$

no sistema de numeração decimal.

$$10^{4033}+10^{4032}+\cdots+10^{2019}+10^{2018}+2.10^{2017}+10^{2016}+\cdots+10+1 \tag{6.4}$$

Podemos reescrever (6.4) *do seguinte modo*

$$10^{2018}\left(\frac{10^{2016}-1}{9}\right)+\left(\frac{10^{2016}-1}{9}\right)+2.10^{2017}$$

que é equivalente a:

$$\begin{aligned}\frac{10^{2018}.10^{2016}-10^{2018}+10^{2016}-1+18.10^{2017}}{9} &= \frac{10^{2016}}{9}\left(10^{2018}-10^2+1+18.10\right)-\frac{1}{9}\\ &= \frac{10^{2016}}{9}\left(10^{2018}-81\right)-\frac{1}{9}\end{aligned}$$

Portanto, o número

$$\underbrace{11\ldots1}_{2016}2\underbrace{11\ldots1}_{2016}$$

é divisível por 9*, logo é composto.* ■

Problema 6.8 ***(Banco de Questões OBMEP - 2017, pg.*** 98***)*** *Uma fração é dita irredutível quando seu numerador e seu denominador não possuem fatores comuns, ou seja, quando o máximo divisor comum entre os dois números é* 1*. Por exemplo, a fração* $\frac{3}{7}$ *é irredutível, mas a fração* $\frac{10}{14}$ *não é, uma vez que* 2 *é um fator comum de* 10 *e* 14*. Para que valores de n a fração* $\frac{5n+6}{6n+5}$ *é irredutível? Vamos estudar esse problema em partes:*

(a) Seja $d=(5n+6,6n+5)$ *o máximo divisor comum de* $5n+6$ *e* $6n+5$*. Verifique se d é um divisor de* $n-1$*.*

(b) Sabendo que d é um divisor de $n-1$*, conclua que d também é um divisor de* 11*.*

(c) Verifique que se 11 *divide* $5n+6$*, então* 11 *divide* $6n+5$*.*

(d) Para quantos inteiros positivos n, menores que 50*, a fração* $\frac{5n+6}{6n+5}$ *é irredutível?*

Solução 6.8 *(a) Neste caso, temos que* $d = (5n+6, 6n+5)$*. Aplicando o* ***Lema de Euclides****, temos*

$$\begin{aligned} d = (5n+6, 6n+5) &= (6n+5, 5n+6) \\ &= (5n+6, 6n+5-(5n+6)) \\ &= (5n+6, 6n+5-5n-6) \\ &= (5n+6, n-1). \end{aligned}$$

Portanto, d divide $n-1$*.*

(b) Pelo item (a) sabemos que $d = (5n+6, n-1)$*, então aplicando o* ***Lema de Euclides*** *novamente temos que*

$$\begin{aligned} d = (5n+6, n-1) &= (n-1, 5n+6) \\ &= (n-1, 5n+6-5(n-1)) \\ &= (n-1, 5n+6-5n+5) \\ &= (n-1, 11). \end{aligned}$$

Logo, d também divide 11*.*

(c) Se 11 *divide* $5n+6$*, então existe* $k \in \mathbb{Z}$ *tal que* $5n+6 = 11k$*. Além disso, podemos escrever* 11 *como*

$$\begin{aligned} 11 &= (6n+5) - 6(n-1) \\ &= (6n+5) - 6[(6n+5) - (5n+6)] \\ &= -5(6n+5) + 6(5n+6) \\ &= -5(6n+5) + 6.11k \\ &= -5(6n+5) + 66k. \end{aligned}$$

O que implica,

$$\begin{aligned} 5(6n+5) &= 66k - 11 \\ &= 11(6k-1). \end{aligned}$$

Como $(5, 11) = 1$ *então, podemos concluir que* 11 *divide* $6n+5$*.*

(d) Neste caso, basta aplicar novamente o ***Lema de Euclides*** *e determinar para quais valores*

de n menores que 50 *a fração* $\frac{5n+6}{6n+5}$ *é irredutível, ou seja, tem* $d = (5n+6, 6n+5) = 1$.

$$\begin{aligned} d = (5n+6, 6n+5) &= (6n+5, 5n+6) \\ &= (5n+6, 6n+5-(5n+6)) \\ &= (5n+6, 6n+5-5n-6) \\ &= (5n+6, n-1) \\ &= (n-1, 5n+6-5(n-1)) \\ &= (n-1, 11). \end{aligned}$$

Note que, se $n \in \{1, 12, 23, 34, 45\}$*, então* $d = 11$*, ou seja, a fração* $\frac{5n+6}{6n+5}$ *é irredutível para* 45 *números inteiros positivos n menores que* 50*.*

■

Problema 6.9 ***(Banco de Questões OBMEP - 2017, pg.*** 102*)*** *Suponha que desejamos encontrar todos os inteiros não negativos x e y que satisfazem a equação*

$$7x + 11y = 154$$

Se usarmos apenas que $7x \leq 154$ *implica* $x \leq 22$ *e testarmos as possibilidades, faremos* 23 *testes de casos! Por outro lado, podemos reescrever a equação como*

$$11y = 154 - 7x = 7(22 - x).$$

Veja que 11 *divide* $7(22-x)$*, mas não possui fatores em comum com o* 7*. Consequentemente* 11 *é um divisor de* $22 - x$*. Como* $22 - x \leq 22$*, basta testar* $x = 0$*,* $x = 11$ *ou* $x = 22$ *para encontrarmos as três soluções* $(x, y) = (0, 14)$*,* $(11, 7)$ *ou* $(22, 0)$ *com apenas três testes de casos. Encontre todos os pares* (m, n) *de inteiros não negativos que satisfazem a equação*

$$5m + 8n = 120.$$

Solução 6.9 *Observe que, no enunciado da problema mostra-se como obter os inteiros não negativos x e y que satisfazem a equação* $7x + 11y = 154$*. Porém, para encontrarmos os pares* (m, n) *de inteiros não negativos que satisfazem a equação* $5m + 8n = 120$ *vamos utilizar os teoremas sobre* ***Equações Diofantinas*** *estudados anteriormente. Note que a equação*

$$5m + 8n = 120 \tag{6.5}$$

possui solução, pois o $(5, 8) = 1 | 120$ *. Uma solução particular para* (6.5) *pode ser dada por*

$x_0 = 8$ *e* $y_0 = 10$. *Assim, podemos escrever a solução geral de* (6.5) *da seguinte forma:*

$$\begin{cases} x &= x_0 + bt \\ y &= y_0 - at \end{cases} \Rightarrow \begin{cases} x &= 8 + 8t \\ y &= 10 - 5t \end{cases} , t \in \mathbb{Z}.$$

Queremos os pares (m,n) *de inteiros não negativos, então*

$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases} \Rightarrow \begin{cases} 8+8t \geq 0 \\ 10-5t \geq 0 \end{cases} \Rightarrow \begin{cases} t \geq -1 \\ t \leq 2 \end{cases} \Rightarrow t \in \{-1,0,1,2\}.$$

Então,

- *para* $t = -1$, *temos o par* $(0,15)$;
- *para* $t = 0$, *temos o par* $(8,10)$;
- *para* $t = 1$, *temos o par* $(16,5)$;
- *para* $t = 2$, *temos o par* $(24,0)$.

Portanto, os pares (m,n) *de inteiros não negativos que satisfazem a equação* (6.5) *são:* $(0,15)$, $(8,10)$, $(16,5)$, $(24,0)$. ■

Problema 6.10 ***(Banco de Questões OBMEP - 2017, pg.*** 121*)*** *Quantos divisores de* 88^{10} *deixam resto* 4 *quando divididos por* 6*?*

Solução 6.10 *Decompondo* 88 *em fatores primos, temos que*

$$88 = 2^3.11 \Rightarrow 88^{10} = (2^3.11)^{10} = 2^{30}.11^{10}.$$

Chamando o expoente de 11 *de m e o de* 2 *de n, os divisores de* 88^{10}*, são da forma*

$$11^m.2^n, \;\; 0 \leq m \leq 10 \;\; e \;\; 0 \leq n \leq 30. \tag{6.6}$$

Aplicando a congruência módulo 6 *em* (6.6)*, obtemos*

$$11^m.2^n \equiv (-1)^m.2^n (mod\ 6). \tag{6.7}$$

Agora, analisando as potências de 2 *módulo* 6*, tem-se*

$$2^1 \equiv 2(mod\ 6) \Rightarrow 2^2 \equiv 4(mod\ 6) \Rightarrow 2^3 \equiv 2(mod\ 6) \Rightarrow 2^4 \equiv 4(mod\ 6)$$

note que, se o expoente é par, será congruente a $4(mod\ 6)$ *e se o expoente é ímpar, será congruente a* $2(mod\ 6)$*, que por sua vez é congruente a* $-4(mod\ 6)$.

Voltando a congruência em (6.7)*, vamos analisar os casos em que m e n são impares, ou seja,*

(i) $0 \leq m \leq 10 \Rightarrow 0 \leq 2k+1 \leq 10 \Rightarrow -1 \leq 2k \leq 9 \Rightarrow 0 \leq k \leq 4.$

(ii) $0 \leq n \leq 30 \Rightarrow 0 \leq 2k'+1 \leq 30 \Rightarrow -1 \leq 2k' \leq 29 \Rightarrow 0 \leq k' \leq 14.$

De acordo com os itens (i) *e* (ii)*, temos* 5 *casos para m e* 15 *para n, logo, temos* $5.15 = 75$ *divisores de* 88^{10} *que deixam resto* 4 *quando divididos por* 6*.*

Agora, vejamos os casos em que m e n são pares. Como são 5 *casos para m ímpar, então temos* 6 *casos para m par, e como são* 15 *casos para n ímpar, então são* 16 *casos para n par, porém, não podemos contar o caso quando* $n = 0$*, ou seja, temos* 15 *casos. Assim, temos* $6.15 = 90$ *divisores de* 88^{10} *que deixam resto* 4 *quando divididos por* 6*, com m e n pares.*

Portanto, o número de divisores de 88^{10} *que deixam resto* 4 *quando divididos por* 6 *é* $75+90 = 165$*.* ■

Problema 6.11 ***(POTI)*** *Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau; quando sobe de três em três degraus, sobram dois degraus e quando sobe de cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre* 150 *e* 200*?*

Solução 6.11 *Seja x o número de degraus da escada. Pelos dados do problema podemos montar o seguinte sistema:*

$$\begin{cases} x & \equiv & 1(mod\ 2) \\ x & \equiv & 2(mod\ 3) \\ x & \equiv & 3(mod\ 5) \end{cases} \tag{6.8}$$

como $(2,3) = (2,5) = (3,5) = 1$*, então podemos aplicar o* ***Teorema Chinês dos Restos****. Note que*

$$n_1 = 2,\ \ n_2 = 3,\ \ n_3 = 5 \ \ e \ \ n = n_1.n_2.n_3 = 2.3.5 = 30$$

por outro lado,

$$N_1 = \frac{n}{n_1} = \frac{30}{2} = 15,\ \ N_2 = \frac{n}{n_2} = \frac{30}{3} = 10 \ \ e \ \ N_3 = \frac{n}{n_3} = \frac{30}{5} = 6.$$

Agora, vamos determinar os inteiros r_i, s_i *com* $i = 1,2,3$ *tais que,* $r_iN_i + s_in_i = 1$*.*

(i) $r_1N_1 + s_1n_1 = 1 \Rightarrow r_1.15 + s_1.2 = 1 \Rightarrow r_1 = 1 \ \ e \ \ s_1 = -7.$

(ii) $r_2N_2 + s_2n_2 = 1 \Rightarrow r_2.10 + s_2.3 = 1 \Rightarrow r_2 = 1 \ \ e \ \ s_2 = -3.$

(iii) $r_3N_3 + s_3n_3 = 1 \Rightarrow r_3.6 + s_3.5 = 1 \Rightarrow r_3 = 1 \ \ e \ \ s_3 = -1.$

Como $c_1 = 1, c_2 = 2$ *e* $c_3 = 3$*, então uma solução para o sistema em* (6.8) *pode ser dada por:*

$$x_0 = c_1r_1N_1 + c_2r_2N_2 + c_3r_3N_3 = 1.1.15 + 2.1.10 + 3.1.6 = 15 + 20 + 18 = 53$$

logo, a solução geral do sistema (6.8) *pode ser expressa da seguinte forma*

$$x = 53 + 30t, \ \ t \in \mathbb{N}.$$

Como x está entre 150 *e* 200*, temos*

$$150 < 53 + 30t < 200 \Rightarrow 97 < 30t < 147 \Rightarrow 3 < t < 5 \Rightarrow t = 4.$$

Portanto, o número de degraus da escada é $x = 53 + 30.4 = 53 + 120 = 173.$ ■

Problema 6.12 ***(POTI)*** *Mostre que existe um número da forma*

$$1\underbrace{99\ldots99}_{n \text{ noves}}1$$

Com $n > 2$*, que é múltiplo de* 1991*.*

Solução 6.12 *Temos*

$$1\underbrace{99\ldots99}_{n \text{ noves}}1 = 2\underbrace{000\ldots00}_{n+1} - 9 = 2.10^{n+1} - 9 = 2000.10^{n-2} - 9.$$

Como $2000 \equiv 9 (mod\ 1991)$*, teremos*

$$1\underbrace{99\ldots99}_{n \text{ noves}}1 \equiv 9.10^{n-2} - 9 \equiv 9(10^{n-2} - 1) (mod\ 1991).$$

Para chegar ao objetivo desejado, precisamos que $9(10^{n-2} - 1) \equiv 0 (mod\ 1991)$ *e como* $(9, 1991) = 1$*, basta que* $10^{n-2} - 1 \equiv 0 (mod\ 1991)$ *o que implica* $10^{n-2} \equiv 1 (mod\ 1991)$*. Como* $(181, 10) = 1$ *e* $(11, 10) = 1$*, usando o* ***Pequeno Teorema de Fermat*** *concluímos que:*

$$\begin{cases} 10^{180} & \equiv & 1 (mod\ 181) \\ 10^{10} & \equiv & 1 (mod\ 11) \Rightarrow 10^{180} \equiv 1 (mod\ 11) \ . \end{cases}$$

Segue que $10^{180} - 1$ *é múltiplo comum de* 181 *e* 11 *e, portanto, múltiplo do mínimo múltiplo comum de* 11 *e* 181 *que é igual a* $11.181 = 1991$*. Daí resulta que, para* $n - 2 =$

$180 \Rightarrow n = 182$ *que*

$$1\underbrace{99\ldots99}_{182}1 \equiv 9(10^{180}-1) \equiv 0(mod\ 1991).$$

■

Problema 6.13 ***(POTI)*** *Os números* 2726, 4472, 5054, 6412 *deixam o mesmo resto na divisão por algum número natural m de dois algarismos. Qual o valor de m?*

Solução 6.13 *Seja r o resto quando os números* 2726, 4472, 5054 *e* 6412 *são divididos por m, então podemos escrever*

$$\begin{cases} 2726 \equiv r(mod\ m) \\ 4472 \equiv r(mod\ m) \\ 5054 \equiv r(mod\ m) \\ 6412 \equiv r(mod\ m) \end{cases} \Rightarrow \begin{cases} 4472 \equiv 2726(mod\ m) \\ 6412 \equiv 5054(mod\ m) \end{cases} \Rightarrow \begin{cases} 1746 \equiv 0(mod\ m) \\ 1358 \equiv 0(mod\ m) \end{cases}$$

então $1746 \equiv 1358(mod\ m)$*, portanto* $1746 - 1358 \equiv 0(mod\ m) \Rightarrow 388 \equiv 0(mod\ m)$*, ou melhor,* $m|388 = 2^2.97$ *e como m possui dois algarismos, devemos ter* $m = 97$*.* ■

Problema 6.14 ***(POTI)*** *Quantos quadrados perfeitos existem entre* 40000 *e* 640000 *que são múltiplos simultaneamente de* 3, 4 *e* 5*?*

Solução 6.14 *Seja k um número quadrado perfeito entre* 40000 *e* 640000*, múltiplos de* 3, 4 *e* 5*. Então k deve ter a forma*

$$k = 3^2.4.5^2.q^2$$

onde q é um número inteiro positivo.

Observe que, como k é um quadrado perfeito, todos os números primos que fazem parte dele devem ter como expoente um número par. No caso do 3 *e do* 5 *temos expoentes pares, mas no caso do* 4*, ele é igual a* 2^2*, e assim, o fator primo é o número* 2*. Já o número q concentra todos os outros números primos, que devem necessariamente estar em uma quantidade par dentro do número k. Como*

$$\begin{aligned} 40000 < k < 640000 &\Rightarrow 40000 < 3^2.4.5^2.q^2 < 640000 \\ &\Rightarrow 200 < 2.3.5.q < 800 \\ &\Rightarrow \frac{20}{3} < q < \frac{80}{3} \\ &\Rightarrow 7 \leq q \leq 26. \end{aligned}$$

Portanto, $q \in [7,26]$*, que possui* $26-7+1 = 20$ *valores possíveis, ou seja, existem* 20 *quadrados perfeitos entre* 40000 *e* 640000*.* ■

Problema 6.15 ***(POTI)*** *Prove que*

$$\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}$$

é um número inteiro para todo $n \in \mathbb{Z}$.

Solução 6.15 *Note que*

$$\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}=\frac{3n^5+5n^3+7n}{15},$$

então, basta mostrar que o numerador é múltiplo de 15. *Pelo* ***Pequeno Teorema de Fermat****, temos:*

$$\left\{\begin{array}{l} n^3 \equiv n(mod\ 3) \\ n^5 \equiv n(mod\ 5) \end{array}\right. \Rightarrow \left\{\begin{array}{l} n^3 = n+3k \\ n^5 = n+5s \end{array}\right. ,k,s \in \mathbb{Z}.$$

Portanto,

$$\begin{aligned} 3n^5+5n^3+7n &= 3(n+5s)+5(n+3k)+7n \\ &= 3n+15s+5n+15k+7n \\ &= 15n+15(s+k) \\ &= 15(n+s+k) \end{aligned}$$

é múltiplo de 15. *Logo, concluímos que o número*

$$\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}=\frac{3n^5+5n^3+7n}{15}$$

é inteiro para todo $n \in \mathbb{Z}$. ■

Problema 6.16 ***(POTI)*** *Determine o resto da divisão de* 2^{2002} *por* 101.

Solução 6.16 *Observe inicialmente que* 101 *é primo, pois de acordo com o* ***Crivo de Eratóstenes****,* $\sqrt{101} \cong 10$ *e não existem números diferente de* 1*, menores ou iguais a* 10 *que dividam* 101. *Além disso, como* $101 \nmid 2$*, então podemos aplicar o* ***Pequeno Teorema de Fermat****. Daí,*

$$\begin{aligned} 2^{101-1} \equiv 1(mod\ 101) &\Leftrightarrow 2^{100} \equiv 1(mod\ 101) \\ &\Leftrightarrow (2^{100})^{20} \equiv 1^{20}(mod\ 101) \\ &\Leftrightarrow 2^{2000} \equiv 1(mod\ 101) \\ &\Leftrightarrow 2^2.2^{2000} \equiv 2^2.1(mod\ 101) \\ &\Leftrightarrow 2^{2002} \equiv 4(mod\ 101). \end{aligned}$$

Portanto, o resto da divisão de 2^{2002} *por* 101 *é* 4. ■

Problema 6.17 ***(POTI)*** *Mostre que se n é ímpar, então* n^2-1 *é divisível por* 8.

Solução 6.17 *Seja n um número ímpar, então podemos escrever* $n = 2k+1$, $k \in \mathbb{Z}$. *Então, temos que*

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k = 4k(k+1).$$

Os números k e $k+1$ *são inteiros consecutivos e, portanto, um deles é par. Segue-se que* n^2-1 *tem* 8 *como fator.* ■

Problema 6.18 ***(OCM 2017 - Nível)*** *Mostre que a fração*

$$\frac{21n+4}{14n+3}$$

é irredutível, seja qual for $n \in \mathbb{N}$.

Solução 6.18 *Neste caso, basta mostrar que o* $(21n+4, 14n+3) = 1$. *De fato, pelo* ***Lema de Euclides****,*

$$\begin{aligned}
(21n+4, 14n+3) &= (14n+3, 21n+4) \\
&= (14n+3, 21n+4-(14n+3)) \\
&= (14n+3, 7n+1) \\
&= (7n+1, 14n+3-(7n+1)) \\
&= (7n+1, 7n+2) \\
&= (7n+1, 7n+2-(7n+1)) \\
&= (7n+1, 1) = 1.
\end{aligned}$$

■

Problema 6.19 ***(OCM 2017 - Nível 3)*** *O Lava Jato* ***Sempre Limpo*** *lava carros oferecendo dois tipos de serviços:*

1. *Lavagem simples:* R$ 24,00.
2. *Lavagem completa:* R$ 36,00.

Certo dia, o gerente resolveu fazer uma promoção, dando 20% *de desconto na lavagem simples e* 10% *de desconto na lavagem completa. No dia da promoção, o faturamento foi de* R$ 810,00. *Qual foi o menor número possível de clientes que foram atendidos?*

Solução 6.19 *Sejam x e y o número de lavagens simples e completa respectivamente. Pelos dados do problema podemos montar a seguinte equação:*

$$\begin{aligned}\frac{80}{100}.24x+\frac{90}{100}.36y=810 &\Rightarrow \frac{8}{10}.24x+\frac{9}{10}.36y=810\\ &\Rightarrow 19,2x+32,4y=810\\ &\Rightarrow 192x+324y=8100.\end{aligned}$$

Pelo ***Algoritmo de Euclides****,*

$$\begin{aligned}324 &= 192.1+132\\ 192 &= 132.1+60\\ 132 &= 60.2+12\\ 60 &= 12.5+0\end{aligned}$$

logo, $(192,132)=12$*.*

Daí, dividindo ambos os lados da equação $192x+324y=8100$ *pelo* $(192,132)=12$*, obtemos*

$$16x+27y=675 \tag{6.9}$$

que possui solução, pois $(16,27)=1|675$*.*

Por inspeção, uma solução particular para (6.9) *pode ser dada por* $x_0=0$ *e* $y_0=25$*. Logo, podemos escrever a solução geral de* (6.9) *da seguinte forma:*

$$\begin{cases} x &= x_0+bt \\ y &= y_0-at \end{cases} \Rightarrow \begin{cases} x &= 27t \\ y &= 25-16t \end{cases} ,t\in\mathbb{Z}.$$

Como queremos uma solução nos inteiros não negativos, então

$$\begin{cases} x &\geq 0 \\ y &\geq 0 \end{cases} \Rightarrow \begin{cases} 27t &\geq 0 \\ 25-16t &\geq \end{cases} \Rightarrow \begin{cases} t &\geq 0 \\ t &\leq 1 \end{cases} \Rightarrow t\in\{0,1\}.$$

Então,

- *para* $t=0\Rightarrow x=0$ *e* $y=25$*.*
- *para* $t=1\Rightarrow x=27$ *e* $y=9$*.*

Portanto, o menor número de clientes atendidos foi 25*.* ■

Problema 6.20 ***(OCM 2017 - Nível 3)*** *Juliano desconfia que dado numero natural* $n>1$ *é primo, ou seja, divisível apenas por* 1 *e por si mesmo. Para confirmar sua desconfiança, é*

suficiente que Juliano verifique se n não possui divisor primo

$$A) \leq (n-1) \quad B) \leq \sqrt{n} \quad C) \leq logn \quad D) \leq \sqrt{\frac{n}{2}} \quad E) nda$$

Solução 6.20 *A solução desta questão refere-se ao* ***Crivo de Erastóstenes*** *que diz: se* $n > 1$ *for composto, então n possui, necessariamente, um divisor primo p tal que* $p \leq \sqrt{n}$*. Ou seja, se n não possui divisores diferentes de* 1*, menores ou iguais a* $\sqrt{n}$*, então n é primo.* ■

Capítulo 7

Considerações Finais

Compreende-se que a efetiva aprendizagem em Matemática é uma ferramenta necessária à inclusão do indivíduo na sociedade e percebe-se que compete à escola e ao professor da disciplina o papel de cultivar tais saberes, também com base na realização de projetos que venham contribuir para crescimento pessoal e profissional do aluno. As Olimpíadas de Matemática são hoje um poderoso instrumento que possibilita aprofundar o conhecimento matemático dos estudantes, desenvolver nos alunos algumas habilidades tais como sistematização, generalização, analogia e capacidade de aprender por conta própria ou em colaboração com os colegas, além de incentivar o aprimoramento matemático dos professores.

Iniciamos este material com um breve histórico sobre o surgimento das Olimpíadas Científicas, dando um destaque especial as Olimpíadas de Matemática, com objetivo de oferecer mais informações para professores e estudantes interessados por este tipo de competição. Além disso, passeamos um pouco sobre a história dos protagonistas na Teoria dos Números. Em seguida, enunciamos e demonstramos algumas propriedades e proposições, alguns lemas, corolários e teoremas relacionados à aritmética.

Por fim, desenvolvemos as soluções de questões relacionadas à aritmética, as quais foram extraídas da OBM, OBMEP e OCM, além do Banco de Questões 2017 da OBMEP e do material elaborado pelo POTI. Nestas soluções, foi possível aplicar as definições, as propriedades e os teoremas de conteúdos que não são trabalhados de forma detalhada e efetiva nas aulas de Matemática do ensino básico. Assim, este material tem como objetivo principal auxiliar professores que tenham interesse de preparar seus alunos, na área de aritmética, para as diversas Olimpíadas de Matemática em qualquer âmbito. Este material nos possibilita trabalhar com uma matemática mais formal, visando a aquisição e ampliação dos padrões da aritmética.

O que nos motivou a escolher esse tema foi o engajamento nos programas que visam preparar estudantes para as Olimpíadas de Matemática, tais como OBMEP na Escola[1], Pro-

[1] Voltado para os professores de Matemática das escolas públicas e para os alunos de licenciatura em Matemática, o programa tem como um dos objetivos contribuir para a formação de professores em Matemática estimulando estudos mais aprofundados e a adoção de novas práticas didáticas em suas salas de aula.

grama de Iniciação Científica Jr (PIC)[2] e Polos Olímpicos de Treinamento Intensivo (POTI). De acordo com experiências vivenciadas nestes programas, foi possível perceber a importância e a necessidade de se ensinar uma aritmética mais formal na educação básica.

Assim, concluímos nosso trabalho produzindo um material didático relacionado à aritmética que possa servir de orientação para professores e alunos de escolas públicas e privadas da educação básica, possibilitando o aumento do acesso de alunos a esse conhecimento, ou seja, tornando a Matemática mais acessível aos alunos, resgatando, assim, a sua importância para quem ensina e para quem aprende.

As sub-áreas que compõem uma prova olímpica de Matemática são: *Álgebra*, *Combinatória*, *Geometria* e *Aritmética*. Neste material, trabalhamos apenas alguns tópicos relacionados a aritmética e aplicamos em problemas olímpicos. Neste sentido, acreditamos que seja interessante para futuros estudos, pesquisas relacionadas as outras sub-áreas.

[2]O Programa de Iniciação Científica Jr. (PIC) é um programa que propicia ao aluno premiado em cada edição da OBMEP entrar em contato com interessantes questões no ramo da Matemática, ampliando o seu conhecimento científico e preparando-o para um futuro desempenho profissional e acadêmico.

Referências Bibliográficas

[1] BOYER, C. B. TRAD. GOMIDE, E.,*História da Matemática*, 2ª edição. Editora São Paulo, 1996, p. 258.

[2] CARNEIRO, Emanuel.*Olimpíada de Matemática: Uma porta para o futuro* , II Bienal de SBM 2004.

[3] CARNEIRO, Emanuel; CAMPOS, Onofre; PAIVA, Max. *Olimpíadas Cearenses de Matemática,* 1981 – 2005. Nível Fundamental, 1ª edição. SBM. Rio de Janeiro, 2014.

[4] CARNEIRO, Emanuel; CAMPOS, Onofre; PAIVA, Max. *Olimpíadas Cearenses de Matemática,* 1981 – 2005. Nível Médio, 1ª edição. SBM. Rio de Janeiro, 2014.

[5] HEFEZ, Abramo. *Aritmética*. Coleção PROFMAT, 2ª edição. SBM. Rio de Janeiro, 2016.

[6] KATZ, Vitor J. *História da Matemática*, Fundação Calouste Gulbenkia. São Paulo, 2010, p. 779 à 795.

[7] MEGA, Élio; WATANADE Renate. *Olimpíadas Brasileiras de Matemática,* 1^a *a* 8^a*.: problemas e resoluções.* SBM. Rio de Janeiro, 1998.

[8] MOREIRA, Carlos Gustavo T. de A.; MARTÍNEZ, Fábio E. Brochero; SALDANHA, Nicolau C. *Tópicos de Teoria dos Números*. Coleção PROFMAT, 1ª edição. SBM. Rio de Janeiro, 2012.

[9] MOREIRA, Carlos; MOTTA, Edmilson; TENGAN, Eduardo; AMÂNCIO; Luiz, SALDANHA, Nicolau; RODRIGUES, Paulo. *Olimpíadas Brasileira de Matemática, 9 a 16 a.: problemas e resoluções.* SBM. Rio de Janeiro, 2003.

[10] OLIVEIRA Krerley Irraciel Martins, ; FERNANDES, Adán José Corcho. *Iniciação à Matemática: um curso com problemas e soluções.* 2ª edição. SBM. Rio de Janeiro, 2012.

[11] SHINE, Carlos Yuzo. 21 *Aulas de Matemática Olímpica.* SBM. Rio de Janeiro, 2009.

[12] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. Coleção Matemática Universitária, 3ª edição. IMPA. Rio de Janeiro, 2012.

[13] VIEIRA, Vandenberg Lopes. *Um Curso Básico em Teoria dos Números*. Campina Grande: EDUEPB, São Paulo: Livraria da Física, 2015.

Apêndice A

Primeiro Apêndice

Todos os problemas expostos no capítulo 6 foram resolvidos utilizando a teoria apresentada nos capítulos 4 e 5, esse foi um dos objetivos do nosso trabalho. Porém para resolver tais problemas existem outras técnicas, sendo assim neste Apêndice, indicaremos aonde o leitor poderá encontrar outra solução para cada um desses problemas.

Outras soluções para os problemas do capítulo 4

A.1 ***Problema 4.1***

37^a *Olimpíada Brasileira de Matemática: Gabarito Segunda Fase: Nível* 2*, parte B problema* 2*.*
http://www.obm.org.br/como-se-preparar/provas-e-gabaritos/

A.2 ***Problema 4.2***

38^a *Olimpíada Brasileira de Matemática: Gabarito Primeira Fase: Nível* 2*, problema* 12*.*
http://www.obm.org.br/como-se-preparar/provas-e-gabaritos/

A.3 ***Problema 4.3***

38^a *Olimpíada Brasileira de Matemática: Gabarito Primeira Fase: Nível* 2*, problema* 10*.*
http://www.obm.org.br/como-se-preparar/provas-e-gabaritos/

A.4 ***Problema 4.4***

13^a *Olimpíada Brasileira de Matemática das Escolas Públicas: Gabarito Primeira Fase: Nível* 3*, problema* 6*.*
http://www.obmep.org.br/provas.htm

A.5 ***Problema 4.5***

13^a *Olimpíada Brasileira de Matemática das Escolas Públicas: Gabarito Primeira Fase: Nível* 3*, problema* 9*.*
http://www.obmep.org.br/provas.htm

A.6 ***Problema 4.6***

13^a *Olimpíada Brasileira de Matemática das Escolas Públicas: Gabarito Segunda Fase: Nível* 3*, problema* 1.
http://www.obmep.org.br/provas.htm

A.7 ***Problema 4.7***

Banco de Questões da OBMEP 2017*: Problema* 6*, página* 93.
http://www.obmep.org.br/banco.htm

A.8 ***Problema 4.8***

Banco de Questões da OBMEP 2017*: Problema* 11*, página* 99.
http://www.obmep.org.br/banco.htm

A.9 ***Problema 4.9***

Banco de Questões da OBMEP 2017*: Problema* 14*, página* 102.
http://www.obmep.org.br/banco.htm

A.10 ***Problema 4.10***

Banco de Questões da OBMEP 2017*: Problema* 27*, página* 121.
http://www.obmep.org.br/banco.htm

A.11 ***Problema 4.11***

http://www.profmat-sbm.org.br/wp-content/uploads/sites/23/2016/08/Gabarito_AV3_MA14_2011.pdf

A.12 ***Problema 4.12***

Programa Olímpico de Treinamento Intensivo (POTI).
http://poti.impa.br/index.php/site/material

A.13 ***Problema 4.13***

Programa Olímpico de Treinamento Intensivo (POTI).
http://poti.impa.br/index.php/site/material

A.14 ***Problema 4.14***

Livro: Olimpíadas Brasileiras de Matemática 1^a *a* 8^a*, página* 43.

A.15 ***Problema 4.15***

Livro: Olimpíadas Cearenses de Matemática 1981 *a* 2005*, página* 143.

A.16 ***Problema 4.16***

Programa Olímpico de Treinamento Intensivo (POTI).
http://poti.impa.br/index.php/site/material

A.17 ***Problema 4.17***

Livro: Olimpíadas Brasileiras de Matemática 1^a *a* 8^a*, página* 39.

A.18 ***Problema 4.18***

http://www.ufcg.edu.br/ ocm/index.php/provas-e-gabaritos

A.19 ***Problema 4.19***

http://www.ufcg.edu.br/ ocm/index.php/provas-e-gabaritos

A.20 ***Problema 4.20***

http://www.ufcg.edu.br/ ocm/index.php/provas-e-gabaritos

Apêndice B

Segundo Apêndice

Neste Apêndice, propomos alguns problemas extraídos das duas principais Olimpíadas de Matemática realizadas nacionalmente a OBM e a OBMEP. Além de problemas da Olimpíada Campinense de Matemática (OCM), do Banco de Questões da OBMEP, (edições 2014, 2015 e 2016) e do programa Polos Olímpico de Treinamento Intensivo (POTI). Em seguida, apresentamos dicas de como resolver tais problemas utilizando os teoremas estudados nos capítulos 4 e 5.

Problema B.1 ***(OBM 2012 - N2, Primeira Fase)*** *Qual é a maior potência de* 2 *que divide* $2011^{2012} - 1$*?*

A) 2 *B)* 4 *C)* 8 *D)* 18 *E)* 32

Problema B.2 ***(OBM 2012 - N2, segunda Fase)*** *No planeta hexaterra, a base usada é a hexadecimal, base* 16*, ao invés da base decimal mais usada na terra. Para compensar a diferença de dígitos entre a base* 10 *e a base* 16*, usamos letras como dígitos: A, B, C, D, E e F (escritas em ordem crescente). Assim, por exemplo,* $(10)_{16}$ *é na verdade* $(16)_{10}$*,* $(AB)_{16} = 10.16 + 11.1 = 176$ *e* $(FDE)_{16} = 15.16^2 + 4.1 = 3854$*. Determine o valor da soma:*

$$(1)_{16} + (2)_{16} + \cdots + (D)_{16} + (E)_{16} + (F)_{16} + (10)_{16} + \cdots + (100)_{16}.$$

Problema B.3 ***(OBM 2013 - N3, Primeira Fase)*** *Num circo, a atração principal é a Corrida de Pulgas. Duas pulgas,* P_1 *e* P_2*, perfeitamente treinadas, saltam ao longo de uma linha reta, com velocidades constantes, partindo de um mesmo ponto e no mesmo instante. Cada salto da pulga* P_1 *tem alcance m centímetros e cada salto da pulga* P_2 *tem alcance n centímetros, com* $m < n$*, ambos inteiros. Porém a pulga* P_1 *é mais rápida que a pulga* P_2*, de modo que, independente da velocidade de* P_2*,* P_1 *sempre pode alcançá-la após alguns saltos. Supondo que, após a largada, as pulgas estarão juntas, pela primeira vez, ao final de* 1 *metro, determine o número de pares (m, n) possíveis.*

A) 12 *B)* 24 *C)* 36 *D)* 48 *E)* 100

Problema B.4 ***(OBM 2014 - N2, Primeira Fase)*** *O número de* 5 *dígitos* $\overline{xy26z}$*, em que cada uma das letras representa um dígito, é divisível por* 8, 9 *e* 11*. Qual o valor de* x*?*

Problema B.5 ***(OBM 2014 - N3, Primeira Fase)*** *Uma sequência* x_n *tem como primeiros termos* $x_0 = x_1 = 2$ *e os demais definidos por* $x_{n+2} = 2x_{n+1} + x_n$*. Qual é o dígito das unidades de*

$$x_0 - x_1 + x_2 - x_3 + \cdots - x_{2013} + x_{2014}?$$

A) 0 *B)* 2 *C)* 4 *D)* 6 *E)* 8

Problema B.6 ***(OBM 2015 - N2, Segunda Fase)*** *Qual é o maior inteiro positivo que deixa cinco restos diferentes quando dividido por* $2, 3, 4, 5$ *e* 6*?*

Problema B.7 ***(OBM 2016 - N2, Primeira Fase)*** *O ano de* 2016 *é sabadoso, pois há cinco meses com cinco sábados. Qual será o próximo ano sabadoso?*

A) 2017 *B)* 2019 *C)* 2020 *D)* 2021 *E)* 2022

Problema B.8 ***(Banco de Questões OBMEP - 2016, pg.*** 89***)*** *Qual o resto da divisão de* 2^{2015} *por* 20*? Bom, é difícil fazer esta divisão diretamente usando apenas papel e caneta. Vamos procurar uma maneira de obter tal resposta analisando os restos de potências de* 2 *por* 20 *com a esperança de encontrar algum padrão neles. Qual o resto que* 2^5 *deixa por* 20*?*

$$2^5 = 32 = 1.20 + 12.$$

Sabendo disto, fica fácil saber o resto de 2^6 *por* 20*, pois*

$$2^6 = 2.2^5 = 2.(1.20 + 12) = 2.20 + 24.$$

Dado que 24 *é maior que* 20 *e não pode ser um resto, devemos escrever*

$$2^6 = 3.20 + 4.$$

Podemos estender o argumento anterior concluindo que para saber o resto de 2^{i+1} *por* 20*, basta saber o resto do produto do resto de* 2^i *por* 20*. Desse modo, podemos construir a sequência de potências e restos na divisão por* 20*.*

n	*Resto por 20*
2^1	2
2^2	4
2^3	8
2^4	16
2^5	12
2^6	4

(a) Determine os restos que os números 2^7, 2^{10} *e* 2^{13} *deixam na divisão por* 20.

(b) Sabendo que os restos se repetem de forma periódica, determine o período de repetição, ou seja, o número de restos distintos que ficam se repetindo.

(c) Voltando à pergunta do começo do problema. Qual o resto que 2^{2015} *deixa na divisão por* 20*?*

Problema B.9 ***(Banco de Questões OBMEP - 2015, pg.*** 152***)*** *Seja n um número inteiro positivo. Se, para cada divisor primo p de n, o número* p^2 *não divide n, dizemos então que n é livre de quadrados. Mostre que todo número livre de quadrados tem uma quantidade de divisores que é igual a uma potência de* 2*.*

Problema B.10 ***(Banco de Questões OBMEP - 2015, pg.*** 159***)*** *Dígitos repetidos.*

(a) Usando que

$$\frac{10^n-1}{9} = \underbrace{111\ldots111}_{n}$$

verifique que:

$$\underbrace{111\ldots111}_{4028} = \underbrace{222\ldots222}_{2014} + \underbrace{(333\ldots333)^2}_{2014}.$$

(b) Considere o número de 4028 *dígitos*

$$X = \underbrace{111\ldots111}_{2013}2\underbrace{888\ldots888}_{2012}96.$$

Calcule $\sqrt{X}$*.*

(c) Mostre que o número

$$\underbrace{444\ldots444}_{n\ vezes}\underbrace{888\ldots8889}_{(n\text{-}1)\ vezes}$$

é um quadrado perfeito.

(d) Mostre que o número

$$\underbrace{111\ldots111}_{4028} - \underbrace{222\ldots222}_{2014}$$

é um quadrado perfeito.

Problema B.11 ***(Banco de Questões OBMEP - 2015, pg.*** 157***)*** *Em uma lousa são escritos os* 2014 *inteiros positivos de* 1 *até* 2014*. A operação permitida é escolher dois números a e b, apagá-los e escrever em seus lugares os números* (a,b) *(Máximo Divisor Comum) e* $[a,b]$ *(Mínimo Múltiplo Comum). Essa operação pode ser feita com quaisquer dois números que estão na lousa, incluindo os números que resultaram de operações anteriores. Determine qual a maior quantidade de números que podemos deixar na lousa.*

Problema B.12 ***(Banco de Questões OBMEP - 2014, pg.*** 59***)*** *Carla escreveu no quadro-negro os números inteiros de até . Diana deseja apagar alguns deles de tal modo que ao multiplicar os números restantes o resultado seja um quadrado perfeito.*

(a) Mostre que Diana deve apagar necessariamente os números 11*,* 13*,* 17 *e* 21 *para conseguir seu objetivo.*

(b) Qual a menor quantidade de números que Diana deve apagar para atingir o seu objetivo?

Problema B.13 ***(POTI)*** *Qual o resto na divisão de* $2^{70}+3^{70}$ *por* 13*?*

Problema B.14 ***(POTI)*** *Existe um conjunto B de* 4004 *inteiros positivos tal que, para cada subconjunto A de B com* 2003 *elementos, a soma dos elementos em A não é divisível por* 2003*?*

Problema B.15 ***(POTI)*** *Determine todos os restos possíveis da divisão do quadrado de um número primo com* 120 *por* 120*.*

Problema B.16 ***(POTI)*** *Determinar os inteiros* $n > 2$ *que são divisíveis por todos os primos menores que n.*

Problema B.17 ***(POTI)*** *Encontre um número natural N que, ao ser dividido por* 10*, deixa resto* 9*, ao ser dividido por* 9 *deixa resto* 8*, e ao ser dividio por* 8 *deixa resto* 7*.*

Problema B.18 ***(POTI)*** *Em quantos zeros termina* 1000!*?*

Problema B.19 ***(POTI)*** *Encontre o menor inteiro positivo x tal que*

$$x \equiv 5 (mod\ 7),\ x \equiv (mod\ 11)\ e\ x \equiv 3 (mod\ 13).$$

Problema B.20 ***(OCM 2015 - Nível 3)*** *Se a e b são inteiros consecutivos, mostre que* $a^2 + b^2 + (ab)^2$ *e um quadrado perfeito.*

Problema B.21 ***(OCM 2014 - Nível 3)*** *Sejam a, b e c números ímpares. Mostre que:*

(a) a^2 *deixa resto* 1 *quando dividido por* 4*.*

(b) $a^2+b^2+c^2$ *não é um quadrado perfeito.*

Problema B.22 ***(OCM 2012 - Nível 3)*** *Quantas são as soluções inteiras positivas da equação* $5x+7y = 2012$*?*

Dicas e Soluções

B.1 *Temos que*

$$2011^{2012}-1=(2011^{1006}-1)(2011^{1006}+1)=(2011^{503}+1)(2011^{503}-1)(2011^{1006}+1).$$

Note que, $2011\equiv -1(mod\ 4)$. *Assim,* $2011^{503}-1=(-1)^{503}-1\equiv 2(mod\ 4)$. *Logo, a maior potência de* 2 *que divide* $2011^{503}-1$ *é* 2.

Também temos que $2011^{1006}+1\equiv(-1)^{2006}+1\equiv 2(mod\ 4)$. *Daí, a maior potência de* 2 *que divide* $2011^{1006}+1$ *também é* 2.

Finalmente, $2011\equiv 3(mod\ 8)$, *o que nos dar* $2011^{503}+1\equiv 3^{503}+1\equiv 4(mod\ 8)$, *donde a maior potência de* 2 *que divide*

$$(2011^{503}+1)(2011^{503}-1)(2011^{1006}+1)$$

é $2.2.4=16$.

B.2 *Somando todos os números da forma* $(XY)_{16}$ *com* X *e* Y *variando no conjunto* $\{0,1,2,\ldots,E,F\}$ *obtemos a soma* $(1)_{16}+(2)_{16}+\cdots+(FF)_{16}+(FF)_{16}$. *Cada dígito é somado* 16 *vezes na posição do* X *e* 16 *vezes na posição do* Y. *O aparecimento do dígito* X *corresponde ao valor* $16X$ *na base* 10. *Sendo assim, essa soma vale:*

$$\begin{aligned}16.16(0+1+\cdots+E+F) &= 16(0+1+\cdots+E+F)\\ &= 272(0+1+\cdots+E+F)\\ &= 272.\frac{15.16}{2}\\ &= 32640.\end{aligned}$$

B.3 *Se a pulga* P_1 *deu* k_1 *saltos e a pulga* P_2 *deu* k_2 *saltos, temos:* $k_1m=k_2n$. *Logo,* m *e* n *são divisores de* 100. *Como elas se encontram pela primeira vez em* 1 *metro, então* $[m,n]=100=2^2.5^2$, *logo* $5^2|n$ *ou* $5^2|m$. *Se* $5^2\nmid n$ *então necessariamente* $5^2|m\Rightarrow n\leq 20<25\leq m$, *contrariando* $n>m$. *Logo,* $5^2|n\Leftrightarrow n=25,50$ *ou* 100. *Para* $n=100$, m *pode ser qualquer um dos outros* 8 *divisores de* 100 . *Para* $n=25$ *ou* $n=50$, *temos que* $4|m$, *logo* $m=4$ *ou* $m=20$. *No total, teremos:* $8+2.2=12$.

B.4 *Pelo critério de divisibilidade por* 8, *os três últimos dígitos devem formar um número múltiplo de* 8. *A única opção admissível é* $z=4$. *Pelo critério de divisibilidade por* 11, $(x+2+z)-(y+6)-x-y$ *deve ser divisível por* 11. *Como* x *e* y *são dígitos, a única opção é* $x=y$. *Finalmente, pelo critério de divisibilidade por* 9, $(x+y+2+6+z)=2x+12$ *deve ser divisível por* 9. *O único dígito que satisfaz tal condição é* $x=3$.

B.5 *Considerar apenas o resto dos números na divisão por* 10, *pois estamos interessados apenas no dígito das unidades. Cada número depende dos dois anteriores, então para buscar*

um padrão, basta verificar quando dois números consecutivos aparecerem novamente na sequência.

B.6 *Como* $[2,3,4,5,6] = 60$ *, segue que* $60-1 = 59$ *deixa resto* 1 *na divisão por* 2*, resto* 2 *na divisão por* 3*, resto* 3 *na divisão por* 4*, resto* 4 *na divisão por* 5 *e resto* 5 *na divisão por* 6*.*

Portanto, o menor inteiro positivo x que deixa restos diferentes quando dividido por $2,3,4,5$ *e* 6 *é menor ou igual a* 59*. Claramente x não pode deixar resto* 0 *por* 6*, pois neste caso também deixaria tal resto por* 2 *e* 3*. Como os restos de x na divisão por* $2,3,4$ *e* 5 *são menores ou iguais a* 4*, caso o resto na divisão por* 6 *também seja menor ou igual a* 4*, teremos os* 5 *restos escolhidos dentre os elementos de* $\{0,1,2,3,4\}$*. Para que todos sejam distintos, levando-se em conta que o resto na divisão por* 6 *determina os restos nas divisões por* 2 *e* 3*, a única distribuição de restos possível é x deixar resto* 0 *por* $2,1$ *por* $3,2$ *por* $4,3$ *por* 5 *e* 4 *por* 6*. Assim* $x+2$ *seria múltiplo de* 60 *o menor valor inteiro positivo de x para que isso ocorra é* $[2,3,4,5,6]-2 = 60-2 = 58$*.*

Resta apenas analisarmos se existem soluções menores quando x deixa resto 5 *por* 6*. Podemos listar todos os números menores que* 60 *com tal propriedade:* 5*,* 11*,* 17*,* 23*,* 29*,* 35*,* 41*,* 47*,* 53 *e* 59*. Dentre eles, o menor que deixa todos os restos distintos na divisão por* $2,3,4,5$ *e* 6 *é o número* 35*. Veja que ele é menor que as outras soluções encontradas. Portanto* $x = 35$*.*

B.7 *Note que um mês possui* 4 *ou* 5 *sábados e que* $365 = 7\Delta 52+1$*. Então, um ano possui* 52 *semanas completas e* 1 *ou* 2 *dias extras, dependendo dele ser ou não bissexto. Desse modo, um ano terá* 52 *ou* 53 *sábados e, chamando de x o número de meses com* 5 *sábados, podemos analisar as equações:*

$$\begin{cases} 5x+4(12-x) = 52 \\ 5x+4(12-x) = 53 \end{cases} \Leftrightarrow \begin{cases} x = 4 \\ x = 5 \end{cases}$$

Então, um ano é sabadoso quando possui 53 *sábados e isso acontece quando* 1 *de janeiro é sábado ou quando* 2 *de janeiro é sábado e o ano é bissexto, como acontece com* 2016*. Quando um ano é bissexto, o dia* 1 *de janeiro avança dois dias na semana em relação ao ano anterior e, quando o ano não é bissexto, ele avança apenas um dia na semana também em relação ao ano anterior. Desse modo, podemos montar a tabela a seguir com os dias* 1 *de janeiro dos próximos anos.*

Ano	2016	2017	2018	2019	2020	2021	2022
1 *de jan*	*sexta*	*domingo*	*segunda*	*terça*	*quarta*	*sexta*	*sábado*

Portanto, o próximo ano sabadoso será 2022*.*

B.8 *Note que* $20 = 2^2.5$ *e que* $2^2 | 2^{2015}$*, então basta determinar o resto da divisão de* 2^{2015} *por* 5*. Como* $(2,5) = 1$*, basta aplicar o* ***Teorema de Euler****.*

B.9 *Supondo n um número livre de quadrados e considerando sua fatoração em primos, ou seja, escrevendo n na forma canônica, temos*

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_k^{\alpha k}.$$

Como n é livre de quadrados, os expoentes α_i são todos iguais a 1*, Portanto,*

$$n = p_1.p_2\dots p_k.$$

Para contarmos os divisores de n, basta contarmos quantos números possuem ou não cada um desses primos p_i. Como temos duas possibilidades para cada um desses primos figurar em um divisor, a saber, estar ou não estar na fatoração dele, pelo princípio multiplicativo temos

$$2.2\dots 2 = 2^k.$$

B.10 *(a) Basta colocar* 2 *e* 3 *em evidência e utilizar o fato que*

$$\frac{10^n - 1}{9} = \underbrace{111\dots 111}_{n}.$$

(b) Escreva X da seguinte forma

$$\underbrace{111\dots 111}_{2013}.10^{2015} + 2.10^{2014} + \underbrace{888\dots 888}_{2014} + 8$$

em seguida utiliza o mesmo procedimento do item (a) e por fim determine a raiz de X.

Nos itens (c) e (d) basta seguir os procedimentos dos itens (a) e (b).

B.11 *Neste problema a ideia é pegar pares de números consecutivos a e $a+1$, pois sabemos que dois números consecutivos são sempre primos entre si, assim podemos concluir que o máximo divisor comum de números consecutivos é* 1*. Logo, escolhendo sempre números consecutivos entre os* 2014 *números, teremos a quantidade máxima de números* 1 *que podemos deixar na lousa.*

B.12 *(a) Para melhor analisar o produto desse número devemos decompor* 21! *em fatores primos, utilizando o* ***Teorema de Legendre*** *temos que,* $21! = 2^{18}.3^9.5^4.7^3.11.13.17.19$*.*

Para que um número seja quadrado perfeito, devemos ter expoentes pares em seus fatores primos. Em 21! *os fatores primos* $11, 13, 17$ *e* 19 *só aparecem uma vez, precisam necessariamente ser apagados para que o produto dos números restantes possa ser um quadrado perfeito.*

(b) Analisando a decomposição em fatores primos do número $21!$*, encontramos os fatores primos* $3,7,11,13,17$ *e* 19 *com expoentes ímpares. Assim precisamos apagar além de* 11*,* 13*,* 17 *e* 19*, um* 3 *e um* 7*. Como* $3.7 = 21$ *e queremos a menor quantidade de números apagados devemos apagar* $11,13,17,19$ *e* 21*.*

B.13 *Como* $(2,13) = (3,13) = 1$*,* $13 \nmid 2$ *e* $13 \nmid 3$ *então, basta aplicar o* ***Pequeno Teorema de Fermat****.*

B.14 *Sim. Um exemplo de tal conjunto é a união de um conjunto de* 2002 *inteiros positivos que deixem resto* 0 *com outro conjunto composto por* 2002 *inteiros que deixem resto* 1 *por* 2003*.*

B.15 *Use a fatoração* $120 = 3.5.23$ *e analise a congruência módulo* $3,5$ *e* 8 *separadamente.*

B.16 *Como* $(n,n-1) = 1$*, se* $n-1$ *possui algum fator primo, ele não dividirá n. Assim,* $n-1 < 2$*. Consequentemente não existe tal inteiro.*

B.17 *O que acontece ao somarmos* 1 *ao nosso número? Ele passa a deixar resto* 0 *na divisão por* $10,9$ *e* 8*. Assim, um possível valor para N é* $10.9.8-1$*.*

B.18 *Basta aplicar o* ***Teorema de Legendre*** *e determinar o valor de* $E_5(1000!)$*.*

B.19 *Basta aplicar o* ***Teorema Chinês dos Restos****.*

B.20 *Escreva b em função de a, ou seja, podemos escrever dois números consecutivos da seguinte forma a e* $b = a+1$*.*

B.21 *Como* $(a,4) = 1$*, pois a é ímpar, então basta aplicar o* ***Teorema de Euler****.*

B.22 *Inicialmente verifique se a equação* ***Diofantina*** *em questão possui solução, caso exista, encontre uma solução particular, em seguida encontre a solução geral e por fim analise os casos onde temos soluções positivas.*